

Undergraduate Texts in Mathematics

UTM

John Stillwell

Mathematics and Its History

A Concise Edition



Springer

Undergraduate Texts in Mathematics

Undergraduate Texts in Mathematics

Series Editors

Sheldon Axler

San Francisco State University, San Francisco, CA, USA

Kenneth Ribet

University of California, Berkeley, CA, USA

Advisory Board

Colin Adams, *Williams College, Williamstown, MA, USA*

L. Craig Evans, *University of California, Berkeley, CA, USA*

Pamela Gorkin, *Bucknell University, Lewisburg, PA, USA*

Roger E. Howe, *Yale University, New Haven, CT, USA*

Michael E. Orrison, *Harvey Mudd College, Claremont, CA, USA*

Lisette G. de Pillis, *Harvey Mudd College, Claremont, CA, USA*

Jill Pipher, *Brown University, Providence, RI, USA*

Jessica Sidman, *Mount Holyoke College, South Hadley, MA, USA*

Undergraduate Texts in Mathematics are generally aimed at third- and fourth-year undergraduate mathematics students at North American universities. These texts strive to provide students and teachers with new perspectives and novel approaches. The books include motivation that guides the reader to an appreciation of interrelations among different aspects of the subject. They feature examples that illustrate key concepts as well as exercises that strengthen understanding.

More information about this series at <http://www.springer.com/series/666>

John Stillwell

Mathematics and Its History

A Concise Edition



Springer

John Stillwell
Department of Mathematics
University of San Francisco
San Francisco, CA, USA

ISSN 0172-6056 ISSN 2197-5604 (electronic)
Undergraduate Texts in Mathematics
ISBN 978-3-030-55192-6 ISBN 978-3-030-55193-3 (eBook)
<https://doi.org/10.1007/978-3-030-55193-3>

Mathematics Subject Classification: 00A05, 00A66, 01A05

© Springer Nature Switzerland AG 2020

This textbook is an abridged and updated version of the author's 'Mathematics and Its History, Third Edition' © Springer Science+Business Media, LLC 2010

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To my grandchildren, Ida and Isaac

Preface

This book is a condensed version of my *Mathematics and Its History*, which has reached a third edition and is now too encyclopedic/overweight to be covered in a single course. Since I feel strongly that a single course overview of undergraduate mathematics is more desirable today than ever before, I have decided to cut *Mathematics and Its History* down to size. Hopefully, this will also make the book more cohesive, with everything connected to everything else. What I said in the Preface to the first edition still applies:

One of the disappointments experienced by most mathematics students is that they never get a course on mathematics. They get courses in calculus, algebra, topology, and so on, but the division of labor in teaching seems to prevent these different topics from being combined into a whole. In fact, some of the most important and natural questions are stifled because they fall on the wrong side of topic boundary lines. Algebraists do not discuss the fundamental theorem of algebra because “that’s analysis” and analysts do not discuss Riemann surfaces because “that’s topology,” for example. Thus if students are to feel they really know mathematics by the time they graduate, there is a need to unify the subject.

This book aims to give a unified view of undergraduate mathematics by approaching the subject through its history. Since readers should have had some mathematical experience, cer-

tain basics are assumed and the mathematics is not developed formally as in a standard text. On the other hand, the mathematics is pursued more thoroughly than in most general histories of mathematics, because mathematics is our main goal and history only the means of approaching it. Readers are assumed to know basic calculus, algebra, and geometry, to understand the language of set theory, and to have met some more advanced topics such as group theory, topology, and differential equations. I have tried to pick out the dominant themes of this body of mathematics, and to weave them together as strongly as possible by tracing their historical development.

Some historians of mathematics may object to my anachronistic use of modern notation and (fairly) modern interpretations of classical mathematics. This has certain risks, such as making the mathematics look simpler than it really was in its time, but the risk of obscuring ideas by cumbersome, unfamiliar notation is greater, in my opinion. Indeed, it is practically a truism that mathematical ideas generally arise before there is notation or language to express them clearly, and that ideas are implicit before they become explicit. Thus the historian, who is presumably trying to be both clear and explicit, often has no choice but to be anachronistic when tracing the origins of ideas.

Mathematicians may object to my choice of topics, since a book of this size is necessarily incomplete. My preference has been for topics with elementary roots and strong interconnections. The major themes are the concepts of number and space: their initial separation in Greek mathematics, their union in the geometry of Fermat and Descartes, and the fruits of this union in calculus and analytic geometry. Certain important topics of today, such as Lie groups and functional analysis, are omitted on the grounds of their comparative remoteness from elementary roots. Others, such as probability theory, are mentioned only briefly, as most of their development seems to have occurred outside the mainstream. For any other omissions or slights I can only plead personal taste and a desire to keep the book within the bounds of a one- or two-semester course.

I would only add that I am hoping in fact to stay within the bounds of a *one*-semester course. Thus the content is now somewhat less than in the first edition of *Mathematics and Its History*, or at least more compact. In particular, I have dropped the biographical sketches that took up about 20% of the book, since short mathematical biographies are now widely available at sites such as

<http://www-history.mcs.st-and.ac.uk/BiogIndex.html>

On the other hand, there are many more exercises than in the first edition, so instructors will have considerable freedom in assigning problems. Also, many of the black-and-white line drawings from earlier editions have been improved or completely replaced by new ones with color, and in many cases with 3D modeling using the excellent free software POV-Ray. These enhancements should make the diagrams easier to “read.”

Much of the material in this condensed version is taken from the full *Mathematics and Its History*, Stillwell (2010a). However, most of Chapter 16 is new, and there are several new sections or subsections in other chapters. In addition, hundreds of small changes and additions have been made to improve clarity and to add new information.

As always, I thank my wife Elaine for her meticulous proofreading. I also thank the anonymous referees for numerous corrections and improvements, and Loretta Bartolini for expertly coordinating the production of the book. Many thanks also go to Rossella Lupacchini for locating a crucial picture in a Bombelli manuscript in Bologna.

John Stillwell

South Melbourne, June 2020

San Francisco, September 2019

Contents

Preface	vii
1 The Theorem of Pythagoras	1
1.1 Arithmetic and Geometry	2
1.2 Pythagorean Triples	4
1.3 Rational Points on the Circle	6
1.4 Right-Angled Triangles	10
1.5 Irrational Numbers	12
2 Greek Geometry	17
2.1 The Deductive Method	18
2.2 The Regular Polyhedra	20
2.3 Ruler and Compass Constructions	23
2.4 Conic Sections	26
2.5 Higher-Degree Curves	29
3 Greek Number Theory	35
3.1 The Role of Number Theory	36
3.2 Polygonal, Prime, and Perfect Numbers	36
3.3 The Euclidean Algorithm	39
3.4 Pell's Equation	43
3.5 The Chord and Tangent Methods	47

4	Infinity in Greek Mathematics	51
4.1	Fear of Infinity	52
4.2	Eudoxus's Theory of Proportions	54
4.3	The Method of Exhaustion	56
4.4	The Area of a Parabolic Segment	60
5	Polynomial Equations	63
5.1	Algebra	64
5.2	Linear Equations and Elimination	65
5.3	Quadratic Equations	68
5.4	Quadratic Irrationals	71
5.5	The Solution of the Cubic	73
5.6	Angle Division	75
5.7	Higher-Degree Equations	77
5.8	The Binomial Theorem	79
5.9	Fermat's Little Theorem	82
6	Algebraic Geometry	85
6.1	Steps Toward Algebraic Geometry	86
6.2	Fermat and Descartes	87
6.3	Algebraic Curves	89
6.4	Newton's Classification of Cubics	91
6.5	Construction of Equations, Bézout's Theorem	94
6.6	The Arithmetization of Geometry	96
7	Projective Geometry	99
7.1	Perspective	100
7.2	Anamorphosis	103
7.3	Desargues's Projective Geometry	105
7.4	The Projective View of Curves	108
7.5	The Projective Plane	112
7.6	The Projective Line	115
7.7	Homogeneous Coordinates	118
8	Calculus	123
8.1	What Is Calculus?	124
8.2	Early Results on Areas and Volumes	125
8.3	Maxima, Minima, and Tangents	128

8.4	The <i>Arithmetica Infinitorum</i> of Wallis	130
8.5	Newton's Calculus of Series	133
8.6	The Calculus of Leibniz	136
9	Infinite Series	139
9.1	Early Results	140
9.2	From Pythagoras to Pi	143
9.3	Power Series	146
9.4	Fractional Power Series	149
9.5	Summation of Series	151
9.6	The Zeta Function	153
10	Elliptic Curves and Functions	157
10.1	Fermat's Last Theorem	158
10.2	Rational Points on Cubics of Genus 0	162
10.3	Rational Points on Cubics of Genus 1	165
10.4	Elliptic and Circular Functions	168
10.5	Elliptic Integrals	170
10.6	Doubling the Arc of the Lemniscate	173
10.7	General Addition Theorems	175
10.8	Elliptic Functions	177
11	Complex Numbers and Curves	181
11.1	Impossible Numbers	182
11.2	Cubic Equations	183
11.3	Angle Division	185
11.4	The Fundamental Theorem of Algebra	189
11.5	Roots and Intersections	193
11.6	The Complex Projective Line	196
11.7	Branch Points	200
11.8	Topology of Complex Projective Curves	201
12	Complex Numbers and Functions	205
12.1	Complex Functions	206
12.2	Conformal Mapping	210
12.3	Cauchy's Theorem	212

12.4	Double Periodicity of Elliptic Functions	215
12.5	Elliptic Curves	218
12.6	Uniformization	222
13	Non-Euclidean Geometries	225
13.1	Transcendental Curves	226
13.2	Curvature of Plane Curves	229
13.3	Curvature of Surfaces	232
13.4	Geodesics	235
13.5	The Parallel Axiom	237
13.6	Spherical and Hyperbolic Geometry	240
13.7	Geometry of Bolyai and Lobachevsky	243
13.8	Beltrami's Conformal Models	248
13.9	The Complex Interpretations	252
14	Group Theory	257
14.1	The Group Concept	258
14.2	Subgroups and Quotients	261
14.3	Permutations and Theory of Equations	263
14.4	Permutation Groups	267
14.5	Polyhedral Groups	269
14.6	Groups and Geometries	272
14.7	Combinatorial Group Theory	275
14.8	Finite Simple Groups	279
15	Topology	283
15.1	Geometry and Topology	284
15.2	Polyhedron Formulas of Descartes and Euler	285
15.3	The Classification of Surfaces	287
15.4	Surfaces and Planes	290
15.5	The Fundamental Group	294
16	Commutative Algebra	297
16.1	Linear Algebra	298
16.2	Vector Spaces	299
16.3	Fields	302
16.4	Algebraic Numbers and Algebraic Integers	305
16.5	Rings	308

16.6	Fields as Vector Spaces	311
16.7	Fields of Algebraic Numbers	313
16.8	Ideals	316
16.9	Ideal Prime Factorization	318
17	Sets, Logic, and Computation	323
17.1	Sets	324
17.2	Ordinals	326
17.3	Measure	329
17.4	Axiom of Choice and Large Cardinals	331
17.5	The Diagonal Argument	334
17.6	Computability	335
17.7	Logic and Gödel's Theorem	339
17.8	Provability and Truth	343
	Image Credits	347
	Bibliography	349
	Index	377



1

The Theorem of Pythagoras

PREVIEW

The Pythagorean theorem is the most appropriate starting point for a book on mathematics and its history. It is not only the oldest mathematical theorem, but also the source of three great streams of mathematical thought: numbers, geometry, and infinity.

The number stream begins with *Pythagorean triples*; triples of integers (a, b, c) such that $a^2 + b^2 = c^2$. The geometry stream begins with the interpretation of a^2 , b^2 , and c^2 as squares on the sides of a right-angled triangle with sides a , b , and hypotenuse c . The infinity stream begins with the discovery that $\sqrt{2}$, the hypotenuse of the right-angled triangle whose other sides are of length 1, is an *irrational* number.

These three streams are followed separately through Greek mathematics in Chapters 2, 3, and 4. The geometry stream resurfaces in Chapter 6, where it takes an *algebraic* turn. The basis of algebraic geometry is the possibility of describing points by numbers—their *coordinates*—and the bridge between coordinates and geometry is precisely the Pythagorean theorem, which defines length in terms of coordinates.

The Pythagorean theorem resurfaces in a new algebraic role in Chapter 16. Here it appears in the guise of the *inner product*, which introduces the concepts of length and angle into vector spaces.

1.1 Arithmetic and Geometry

If there is one theorem known to all mathematically educated people, it is surely the theorem of Pythagoras. It will be recalled as a property of right-angled triangles: the square of the hypotenuse equals the sum of the squares of the other two sides (Figure 1.1). The “sum” is of course the sum of areas and the area of a square of side l is l^2 , which is why we call it “ l squared.” Thus the Pythagorean theorem can also be expressed by

$$a^2 + b^2 = c^2, \quad (1)$$

where a, b, c are the side lengths of the red triangle in Figure 1.1.

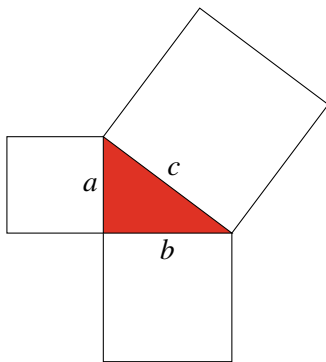


Figure 1.1: The Pythagorean theorem

Conversely, a solution of (1) by positive numbers a, b, c can be realized by a right-angled triangle with sides a, b and hypotenuse c . It is clear that we can draw perpendicular sides a, b for any given positive numbers a, b , and then the hypotenuse c must be a solution of (1) to satisfy the Pythagorean theorem. This converse view of the theorem becomes interesting when we notice that (1) has some very simple solutions. For example,

$$\begin{aligned} (a, b, c) &= (3, 4, 5), & (3^2 + 4^2 &= 9 + 16 = 25 = 5^2), \\ (a, b, c) &= (5, 12, 13), & (5^2 + 12^2 &= 25 + 144 = 169 = 13^2). \end{aligned}$$

It is thought that in ancient times such solutions may have been used for the construction of right angles. For example, by stretching a closed rope with 12 equally spaced knots one can obtain a (3, 4, 5) triangle with right angle between the sides 3, 4, as seen in Figure 1.2.

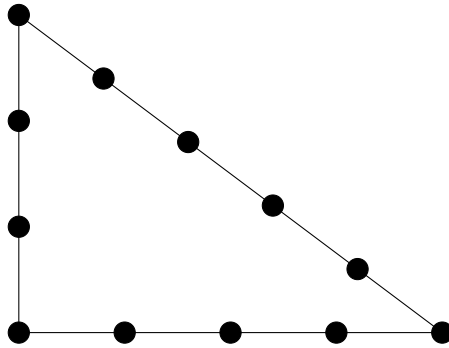


Figure 1.2: Right angle by rope stretching

Whether or not this is a practical method for constructing right angles, the very existence of a geometrical interpretation of a purely arithmetical fact like

$$3^2 + 4^2 = 5^2$$

is quite wonderful. At first sight, arithmetic and geometry seem to be completely unrelated realms. Arithmetic is based on counting, the epitome of a *discrete* (or *digital*) process. The facts of arithmetic can be clearly understood as outcomes of certain counting processes, and one does not expect them to have any meaning beyond this. Geometry, on the other hand, involves *continuous* rather than discrete objects, such as lines, curves, and surfaces. Continuous objects cannot be built from simple elements by discrete processes, and one expects to *see* geometrical facts rather than arrive at them by calculation.

The Pythagorean theorem was the first hint of a hidden, deeper relationship between arithmetic and geometry, and it has continued to hold a key position between these two realms throughout the history of mathematics. This has sometimes been a position of cooperation and sometimes one of conflict, as followed the discovery that $\sqrt{2}$ is irrational (see Section 1.5). It is often the case that new ideas emerge from such areas of tension, resolving the conflict and allowing previously irreconcilable ideas to interact fruitfully. The tension between arithmetic and geometry is, without doubt, the most profound in mathematics, and it has led to the most profound theorems. Since the Pythagorean theorem is the first of these, and the most influential, it is a fitting subject for our first chapter.

1.2 Pythagorean Triples

Pythagoras lived around 500 BCE, but the story of the Pythagorean theorem begins long before that, at least as far back as 1800 BCE in Babylonia. The evidence is a clay tablet, known as Plimpton 322, which systematically lists a large number of integer pairs (a, c) for which there is an integer b satisfying

$$a^2 + b^2 = c^2. \quad (1)$$

A translation of this tablet, together with its interpretation and historical background, was first published by Neugebauer and Sachs (1945). Integer triples (a, b, c) satisfying (1)—for example, $(3, 4, 5)$, $(5, 12, 13)$, $(8, 15, 17)$ —are now known as *Pythagorean triples*. Presumably the Babylonians were interested in them because of their interpretation as sides of right-angled triangles, though this is not known for certain. At any rate, the problem of finding Pythagorean triples was considered interesting in other ancient civilizations that are known to have possessed the Pythagorean theorem; van der Waerden (1983) gives examples from China (between 200 BCE and 220 CE) and India (between 500 and 200 BCE). The most complete understanding of the problem in ancient times was achieved in Greek mathematics, between Euclid (around 300 BCE) and Diophantus (around 250 CE).

A general formula for generating Pythagorean triples is

$$a = (p^2 - q^2)r, \quad b = 2qpr, \quad c = (p^2 + q^2)r.$$

It is easy to see that $a^2 + b^2 = c^2$ when a, b, c are given by these formulas, and of course a, b, c will be integers if p, q, r are. Even though the Babylonians did not have the advantage of our algebraic notation, it is plausible that this formula, or the special case

$$a = p^2 - q^2, \quad b = 2pq, \quad c = p^2 + q^2$$

(which gives all solutions a, b, c , without common divisor and b even) was the basis for the triples they listed. Less general formulas have been attributed to Pythagoras himself (around 500 BCE) and Plato (see Heath (1921), Vol. 1, pp. 80–81); a solution equivalent to the general formula is given in Euclid's *Elements*, Book X (lemma following Prop. 28). As far as we know, this is the first statement of the general solution and the first proof that it is general. Euclid's proof is essentially arithmetical, as one would expect since the problem seems to belong to arithmetic.

However, there is a far more striking solution, which uses the geometric interpretation of Pythagorean triples. This emerges from the work of Diophantus, and it is described in the next section.

EXERCISES

The integer pairs (a, c) in Plimpton 322 are shown in Figure 1.3.

a	c
119	169
3367	4825
4601	6649
12709	18541
65	97
319	481
2291	3541
799	1249
481	769
4961	8161
45	75
1679	2929
161	289
1771	3229
56	106

Figure 1.3: Pairs in Plimpton 322

1.2.1 For each pair (a, c) in the table, compute $c^2 - a^2$, and confirm that it is a perfect square, b^2 . (Computer assistance is recommended.)

You should notice that in most cases b is a “rounder” number than a or c .

1.2.2 Show that most of the numbers b are divisible by 60, and that the rest are divisible by 30 or 12.

Such numbers were in fact exceptionally “round” for the Babylonians, because 60 was the base for their system of numerals. It looks like they computed Pythagorean triples starting with the “round” numbers b and that the column of b values later broke off the tablet.

Euclid’s formula for Pythagorean triples comes out of his theory of divisibility, which we take up in Section 3.3. Divisibility is also involved in some basic properties of Pythagorean triples, such as their evenness or oddness.

1.2.3 Show that any integer square leaves remainder 0 or 1 on division by 4.

1.2.4 Deduce from Exercise 1.2.3 that if (a, b, c) is a Pythagorean triple then a and b cannot both be odd.

1.3 Rational Points on the Circle

We know from Section 1.1 that a Pythagorean triple (a, b, c) can be realized by a triangle with sides a, b and hypotenuse c . This in turn yields a triangle with fractional (or *rational*) number sides $x = a/c, y = b/c$ and hypotenuse 1. All such triangles can be fitted inside the circle of radius 1 as shown in Figure 1.4. The sides x and y become what we now call the *coordinates* of

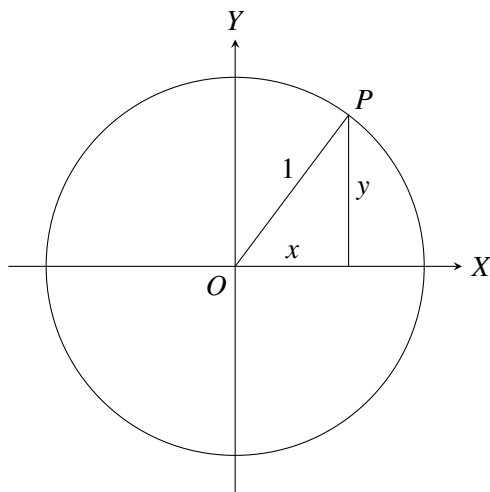


Figure 1.4: The unit circle

the point P on the circle. The Greeks did not use this language, but they could derive the relationship between x and y we call the *equation of the circle*. Since

$$a^2 + b^2 = c^2 \quad (1)$$

we have

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1,$$

so the relationship between $x = a/c$ and $y = b/c$ is

$$x^2 + y^2 = 1. \quad (2)$$

Consequently, finding integer solutions of (1) is equivalent to finding rational solutions of (2), or finding *rational points* on the curve (2).

Such problems are now called *Diophantine*, after Diophantus, who was the first to deal with them seriously and successfully. *Diophantine equations* have acquired the more special connotation of equations for which integer solutions are sought, although Diophantus himself sought only rational solutions. (There is an interesting open problem that turns on this distinction. Matiyasevich (1970) proved that there is no algorithm for deciding which polynomial equations have integer solutions. It is not known whether there is an algorithm for deciding which polynomial equations have *rational* solutions.)

Most of the problems solved by Diophantus involve quadratic or cubic equations, usually with one obvious trivial solution. Diophantus used the obvious solution as a stepping stone to the nonobvious, but no account of his method survived. It was ultimately reconstructed by Fermat and Newton in the 17th century, and this *chord and tangent construction* will be considered later. Here, we need it only for the equation $x^2 + y^2 = 1$, which is an ideal showcase for the method in its simplest form (chord only).

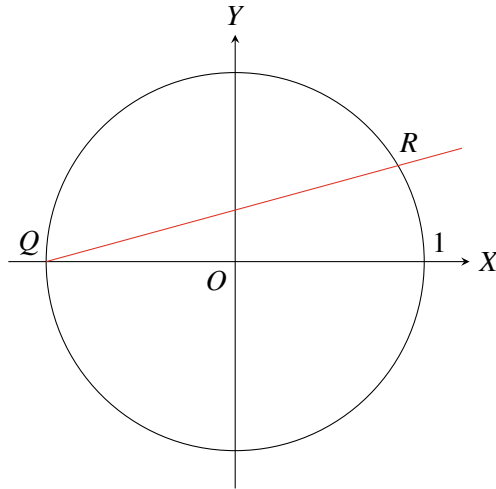


Figure 1.5: Construction of rational points

A trivial solution of this equation is $x = -1, y = 0$, which is the point Q on the unit circle (Figure 1.5). After a moment's thought, one realizes that a line through Q , with rational slope t ,

$$y = t(x + 1) \tag{3}$$

will meet the circle at a second rational point R . This is because substitution of $y = t(x + 1)$ in $x^2 + y^2 = 1$ gives a quadratic equation with rational coefficients and one rational solution ($x = -1$); hence the second solution must also be a rational value of x . But then the y value of this point will also be rational, since t and x will be rational in (3). Conversely, the chord joining Q to any other rational point R on the circle will have a rational slope. Thus by letting t run through all rational values, we find all rational points $R \neq Q$ on the unit circle.

What are these points? We find them by solving the equations just discussed. Substituting $y = t(x + 1)$ in $x^2 + y^2 = 1$ gives

$$x^2 + t^2(x + 1)^2 = 1,$$

or

$$x^2(1 + t^2) + 2t^2x + (t^2 - 1) = 0.$$

This quadratic equation in x has solutions -1 and $(1 - t^2)/(1 + t^2)$. The nontrivial solution $x = (1 - t^2)/(1 + t^2)$, when substituted in (3), gives $y = 2t/(1 + t^2)$.

EXERCISES

The parameter t in the pair $(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$ runs through all rational numbers if $t = q/p$ and p, q run through all pairs of integers.

1.3.1 Deduce that if (a, b, c) is any Pythagorean triple then

$$\frac{a}{c} = \frac{p^2 - q^2}{p^2 + q^2}, \quad \frac{b}{c} = \frac{2pq}{p^2 + q^2}$$

for some integers p and q .

1.3.2 Use Exercise 1.3.1 to prove Euclid's formula for Pythagorean triples, assuming b even. (Remember, a and b are not both odd.)

The triples (a, b, c) in Plimpton 322 seem to have been computed to provide right-angled triangles covering a range of shapes—their angles actually follow a decreasing sequence in roughly equal steps. Figure 1.6 shows the lines with slope a/b , ranging from the top value 119/120 for the top line in Plimpton 322, to 56/90 for the bottom line.

This raises the question, can the shape of any right-angled triangle be approximated by a Pythagorean triple?

1.3.3 Show that any right-angled triangle with hypotenuse 1 may be approximated arbitrarily closely by one with rational sides.

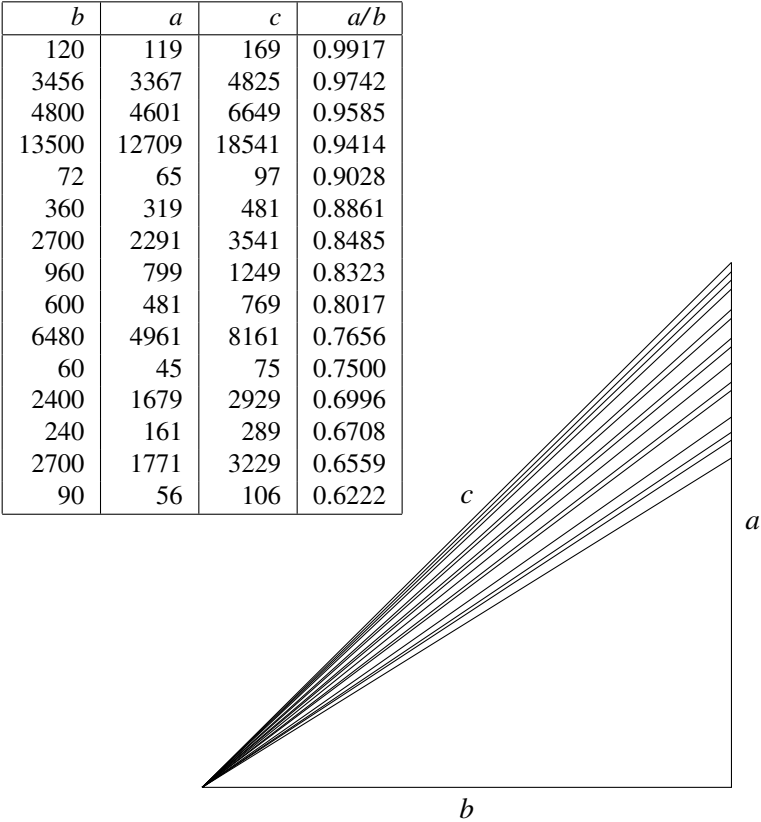


Figure 1.6: Lines of slope a/b corresponding to entries in Plimpton 322

Some important trigonometry may be gleaned from Diophantus’s method if we compare the angle at O in Figure 1.4 with the angle at Q in Figure 1.5. The two angles are shown in Figure 1.7, and high school geometry shows that the angle at Q is half the angle at O .

1.3.4 Why does the angle at Q equal $\theta/2$? (Hint: consider angles in the red triangle.)

1.3.5 Use Figure 1.7 to show that $t = \tan \frac{\theta}{2}$ and

$$\cos \theta = \frac{1 - t^2}{1 + t^2}, \quad \sin \theta = \frac{2t}{1 + t^2}.$$

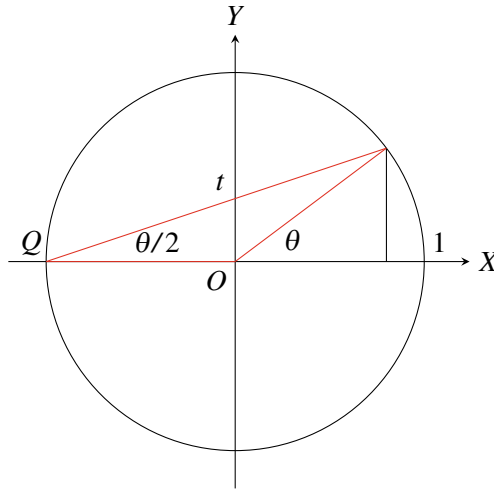


Figure 1.7: Angles in a circle

1.4 Right-Angled Triangles

It is high time we looked at the Pythagorean theorem from the traditional point of view, as a theorem about right-angled triangles; however, we will be rather brief about its proof. It is not known how the theorem was first proved, but probably it was by simple manipulations of area, perhaps suggested by rearrangement of floor tiles. Just how easy it can be to prove the Pythagorean theorem is shown by Figure 1.8, given by Heath (1925) in his edition of Euclid's *Elements*, Vol. 1, p. 354. Each large square contains four copies of the given right-angled triangle. Subtracting these four triangles from the large square leaves, on the one hand (Figure 1.8, *right*), the sum of the squares on the two sides of the triangle. On the other hand (*left*), it also leaves the square on the hypotenuse. This proof, like the hundreds of others that have been given for the Pythagorean theorem, rests on certain geometric assumptions. It is in fact possible to transcend geometric assumptions by using numbers as the foundation for geometry, and the Pythagorean theorem then becomes true almost by definition, as an immediate consequence of the definition of distance (see Section 1.5).

To the Greeks, however, it did not seem possible to build geometry on the basis of numbers, due to a conflict between their notions of number and length. In the next section we will see how this conflict arose.

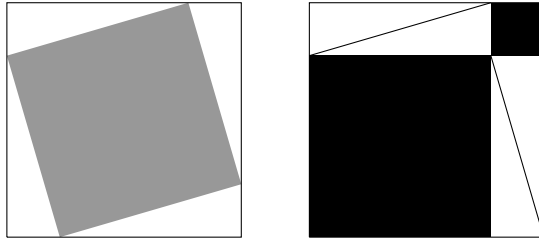


Figure 1.8: Proof of the Pythagorean theorem

EXERCISES

A way to see the Pythagorean theorem in a tiled floor was suggested by Magnus (1974), p. 159, and it is shown in Figure 1.9. (The dotted squares are not tiles; they are a hint.)

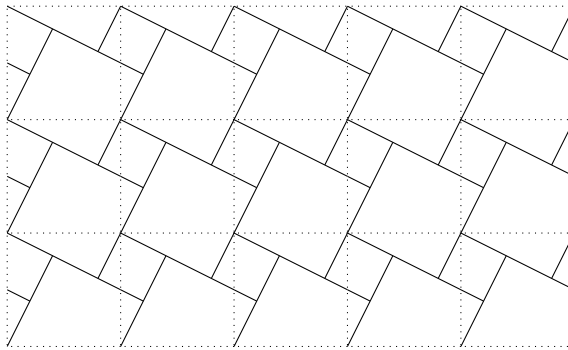


Figure 1.9: Pythagorean theorem in a tiled floor

1.4.1 What has this figure to do with the Pythagorean theorem?

Euclid's first proof of the Pythagorean theorem, in Book I of the *Elements*, is also based on area. It depends only on the fact that triangles with the same base and height have equal area, though it involves a rather complicated figure. In Book VI, Proposition 31, he gives another proof, based on similar triangles (Figure 1.10).

1.4.2 Show that the three triangles in Figure 1.10 are similar, and hence prove the Pythagorean theorem by equating ratios of corresponding sides.

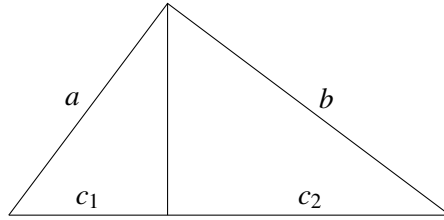


Figure 1.10: Another proof of the Pythagorean theorem

1.5 Irrational Numbers

We have mentioned that the Babylonians, although probably aware of the geometric meaning of the Pythagorean theorem, devoted most of their attention to the whole-number triples it had brought to light, the Pythagorean triples. Pythagoras and his followers were even more devoted to whole numbers. It was they who discovered the role of numbers in musical harmony: dividing a vibrating string in two raises its pitch by an octave, dividing in three raises the pitch another fifth, and so on. This great discovery, the first clue that the physical world might have an underlying mathematical structure, inspired them to seek numerical patterns, which to them meant *whole-number* patterns, everywhere. Imagine their consternation when they found that the Pythagorean theorem led to quantities that were not numerically computable. They found lengths that were *incommensurable*, that is, not measurable as integer multiples of the same unit. The ratio between such lengths is therefore not a ratio of whole numbers, hence in the Greek view not a ratio at all, or *irrational*.

The incommensurable lengths discovered by the Pythagoreans were the side and diagonal of the unit square. It follows immediately from the Pythagorean theorem that

$$(\text{diagonal})^2 = 1 + 1 = 2.$$

Hence if the diagonal and side are in the ratio m/n (where m and n can be assumed to have no common divisor), we have

$$m^2/n^2 = 2,$$

whence

$$m^2 = 2n^2.$$

The Pythagoreans were interested in odd and even numbers, so they probably observed that the latter equation, which says that m^2 is even, also implies that m is even, say $m = 2p$. But if

$$m = 2p,$$

then

$$2n^2 = m^2 = 4p^2;$$

hence

$$n^2 = 2p^2,$$

which similarly implies that n is even, contrary to the hypothesis that m and n have no common divisor. (This proof is in Aristotle's *Prior Analytics*. An alternative, more geometric, proof is mentioned in Section 3.4.)

This discovery had profound consequences. Legend has it that the first Pythagorean to make the result public was drowned at sea (see Heath (1921), Vol. 1, pp. 65, 154). It led to a split between the theories of number and space that was not healed until the 19th century (if then, some believe). The Pythagoreans could not accept $\sqrt{2}$ as a number, but no one could deny that it was the diagonal of the unit square. Consequently, geometrical quantities had to be treated separately from numbers or, rather, without mentioning any numbers except rationals. Greek geometers thus developed ingenious techniques for precise handling of arbitrary lengths in terms of rationals, known as the *theory of proportions* and the *method of exhaustion*.

As we will see in Chapter 4, these techniques made necessary use of *infinity*—something that the Greeks were very reluctant to do.

The Reconciliation of Numbers with Geometry

As we now know, it is not necessary to deny that $\sqrt{2}$ is a number, or to do geometry without applying the processes of arithmetic to lengths, areas, and volumes. In the 1620s, Fermat and Descartes realized that, if lengths are viewed as numbers, then each point P in the plane is given by an ordered pair (x, y) of numbers, called the *coordinates* of P . The coordinates x and y are respectively the horizontal and vertical distances of P from an origin O . We tell the story of their discovery, and the reasons for its success, in Chapter 6.

In coordinate geometry one can *define* the distance between any two points, guided by none other than the Pythagorean theorem. If $P_1 = (x_1, y_1)$

and $P_2 = (x_2, y_2)$ then the line P_1P_2 from P_1 to P_2 is the hypotenuse of a triangle with horizontal side $x_2 - x_1$ and vertical side $y_2 - y_1$ (Figure 1.11).

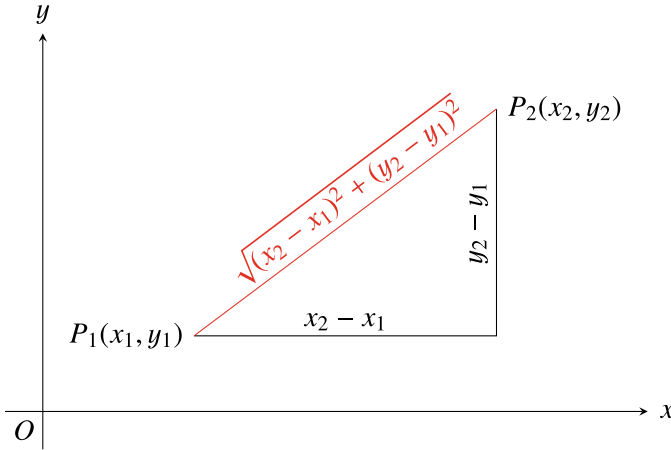


Figure 1.11: Distance via the Pythagorean theorem

Since the square of the hypotenuse is the sum of the squares on the other two sides,

$$(x_2 - x_1)^2 + (y_2 - y_1)^2,$$

we should define

$$\text{length of } P_1P_2 = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}.$$

It follows, for example, that the points (x, y) at distance 1 from O satisfy the equation $x^2 + y^2 = 1$, which we called the *equation of the (unit) circle* in Section 1.3. The coordinate geometry of Fermat and Descartes is part of what is now called *algebraic geometry*, a vast expansion of Greek geometry. Algebraic geometry was made possible by 16th century discoveries in algebra, which brought the study of curves into alignment with the study of polynomial equations.

A coordinate geometry closer in content to Greek geometry, particularly that of Euclid, was developed by Grassmann in the 1840s. Grassmann's geometry is part of what we now call *linear algebra*, and its key concept—the *inner product*—is also inspired by the Pythagorean theorem. For more on linear algebra and the inner product, see Section 16.2.

EXERCISES

The crucial step in the proof that $\sqrt{2}$ is irrational is showing that m^2 even implies m is even or, equivalently, that m odd implies m^2 odd. It is worth taking a closer look at why this is true.

1.5.1 Writing an arbitrary odd number m in the form $2q + 1$, for some integer q , show that m^2 also has the form $2r + 1$, which shows that m^2 is also odd.

You probably did some algebra like this in Exercise [1.2.3](#), but if not, here is your chance:

1.5.2 Show that the square of $2q + 1$ is in fact of the form $4s + 1$, and hence explain why every integer square leaves remainder 0 or 1 on division by 4.



2

Greek Geometry

PREVIEW

Geometry was the first branch of mathematics to become highly developed. The concepts of “theorem” and “proof” originated in geometry, and most mathematicians until recent times were introduced to their subject through the geometry in Euclid’s *Elements*.

In the *Elements* one finds the first system for deriving theorems from supposedly self-evident statements called *axioms*. Euclid’s axioms are incomplete and one of them, the so-called *parallel* axiom, is not as obvious as the others. Nevertheless, it took over 2000 years to produce a clearer foundation for geometry.

The climax of the *Elements* is the investigation of the regular polyhedra, five symmetric figures in three-dimensional space. The five regular polyhedra make several appearances in mathematical history, most importantly in the theory of symmetry—*group theory*—discussed in Chapter 14.

The *Elements* contains not only proofs but also many *constructions*, by ruler and compass. However, three constructions are conspicuous by their absence: duplication of the cube, trisection of the angle, and squaring the circle. These problems were not properly understood until the 19th century, when they were resolved (in the negative) by algebra and analysis.

The only curves in the *Elements* are circles, but the Greeks studied many other curves, such as the conic sections. Again, many problems that the Greeks could not solve were later clarified by algebra. In particular, curves can be classified by *degree*, and the conic sections are the curves of degree 2, as we will see in Chapter 6.

2.1 The Deductive Method

He was 40 years old before he looked on Geometry; which happened accidentally. Being in a Gentleman's Library, Euclid's Elements lay open, and 'twas the 47 El. libri I. He read the Proposition. *By G*—sayd he (he would now and then sweare an emphaticall Oath by way of emphasis) *this is impossible!* So he reads the Demonstration of it, which referred him back to such a Proposition; which proposition he read. That referred him back to another, which he also read . . . that at last he was demonstratively convinced of that trueth. This made him in love with Geometry.

This quotation about the philosopher Thomas Hobbes (1588–1679), from Aubrey's *Brief Lives*, beautifully captures the force of Greece's most important contribution to mathematics, the deductive method. (The proposition mentioned, incidentally, is the Pythagorean theorem.)

We have seen that significant results were *known* before the period of classical Greece, but the Greeks were the first to find results by deduction from previously established results, resting ultimately on the most evident possible statements, called *axioms*. Thales (624–547 BCE) is thought to be the originator of this method (see Heath (1921), p. 128), and by 300 BCE Euclid's *Elements* set the standard for mathematical rigor until the 19th century. But the *Elements* is difficult, so in time it was boiled down to the simplest and driest propositions about lines, angles, and circles. These propositions are based on the following axioms (in the translation of Heath (1925), p. 154), which Euclid called *postulates* and *common notions*.

Postulates

Let the following be postulated:

1. To draw a straight line from any point to any point.
2. To produce a finite straight line continuously in a straight line.
3. To describe a circle with any center and distance.
4. That all right angles are equal to one another.
5. That, if a straight line falling on two straight lines make the interior angles on the same side less than two right angles, the two straight lines, if produced indefinitely, meet on that side on which are the angles less than the two right angles.

Common Notions

1. Things which are equal to the same thing are also equal to one another.
2. If equals be added to equals, the wholes are equal.
3. If equals be subtracted from equals, the remainders are equal.
4. Things which coincide with one another are equal to one another.
5. The whole is greater than the part.

It appears that Euclid's intention was to deduce geometric propositions from visually evident statements (the postulates) using evident principles of logic (the common notions). Actually, he often made unconscious use of visually plausible assumptions that are not among his postulates. His very first proposition used the unstated assumption that two circles meet if the center of each is on the circumference of the other (Heath (1925), p. 242). Nevertheless, such flaws were not noticed until the 19th century, and they were rectified by Hilbert (1899). By themselves, they probably would not have been enough to end the *Elements'* run of 22 centuries as a leading textbook. The *Elements* was overthrown by more serious mathematical upheavals in the 19th century. The so-called non-Euclidean geometries, using alternatives to Euclid's fifth postulate (the *parallel axiom*), developed to the point where the old axioms could no longer be considered self-evident (see Chapter 13). At the same time, the concept of number matured to the point where irrational numbers became acceptable, and indeed preferable to intuitive geometric concepts, in view of the doubts about what the self-evident truths of geometry really were.

The outcome was a more adaptable language for geometry in which "points," "lines," and so on, could be defined, usually in terms of numbers, so as to suit the type of geometry under investigation. Such a development was long overdue. Even in Euclid's time the Greeks were investigating curves more complicated than circles, which did not fit conveniently in Euclid's system. Descartes (1637) introduced the coordinate method, which gives a single framework for handling both Euclid's geometry and higher curves (see Chapter 6), but it was not at first realized that coordinates allowed geometry to be entirely rebuilt on numerical foundations.

The comparatively trivial step (for us) of passing to axioms about numbers from axioms about points had to wait until the 19th century, when geometric axioms about points lost authority and number-theoretic axioms gained it. We say about these developments later (and of problems with the

authority of axioms in general, which arose in the 20th century). For the remainder of this chapter we will look at some important nonelementary topics in Greek geometry, using the coordinate framework where convenient.

EXERCISES

Euclid's Common Notions 1 and 4 define what we now call an *equivalence relation*, which is not necessarily the equality relation. In fact, the kind of relation Euclid had in mind was equality in *some* geometric quantity such as length or angle (but not necessarily equality in all respects—the latter is what he meant by “coinciding”). An equivalence relation \cong is normally defined by three properties. For any a , b and c :

$$\begin{aligned} a &\cong a, && \text{(reflexive)} \\ a \cong b &\Rightarrow b \cong a, && \text{(symmetric)} \\ a \cong b \text{ and } b \cong c &\Rightarrow a \cong c. && \text{(transitive)} \end{aligned}$$

- 2.1.1** Explain how Common Notions 1 and 4 may be interpreted as the transitive and reflexive properties. Note that the natural way to write Common Notion 1 symbolically is slightly different from the statement of transitivity above.
- 2.1.2** Show that the symmetric property follows from Euclid's Common Notions 1 and 4.

Hilbert (1899) took advantage of Euclid's Common Notions 1 and 4 in his rectification of Euclid's axiom system. He *defined* equality of length by postulating a transitive and reflexive relation on line segments, and stated transitivity in the style of Euclid, so that the symmetric property was a consequence.

2.2 The Regular Polyhedra

Greek geometry is virtually complete as far as the elementary properties of plane figures are concerned. It is fair to say that only a handful of interesting elementary propositions about triangles and circles have been discovered since Euclid's time. Solid geometry is much more challenging, even today, so it is understandable that it was left in a less complete state by the Greeks. Nevertheless, they made some very impressive discoveries and managed to complete one of the most beautiful chapters in solid geometry, the enumeration of the regular polyhedra. The five possible regular polyhedra are shown in Figure 2.1. (Images courtesy of Wikimedia.)

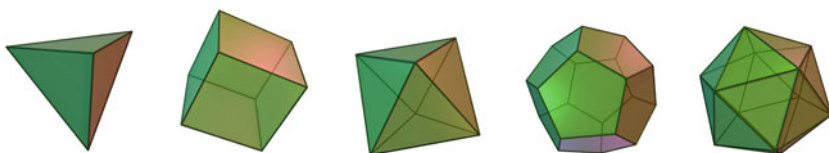


Figure 2.1: Tetrahedron, cube, octahedron, dodecahedron, icosahedron

Each polyhedron is convex and is bounded by a number of congruent polygonal faces, the same number of faces meet at each vertex, and in each face all the sides and angles are equal, hence the term *regular polyhedron*. A regular polyhedron is a spatial figure analogous to a regular polygon in the plane. But whereas there are regular polygons with any number $n \geq 3$ of sides, there are only five regular polyhedra.

This fact is easily proved and may go back to the Pythagoreans (see, for example Heath (1921), p. 159). One considers the possible polygons that can occur as faces, their angles, and the numbers of them that can occur at a vertex. For a 3-gon (triangle) the angle is $\pi/3$, so three, four, or five can occur at a vertex, but six cannot, as this would give a total angle 2π and the vertex would be flat. For a 4-gon the angle is $\pi/2$, so three can occur at a vertex, but not four. For a 5-gon the angle is $3\pi/5$, so three can occur at a vertex, but not four. For a 6-gon the angle is $2\pi/3$, so not even three can occur at a vertex. But at least three faces must meet at each vertex of a polyhedron, so 6-gons (and, similarly, 7-gons, 8-gons, ...) cannot occur as faces of a regular polyhedron. This leaves only the five possibilities just listed, which correspond to the five known regular polyhedra.

But do these five really exist? There is no trouble constructing the tetrahedron, cube, or octahedron, but it is not clear that, say, 20 equilateral triangles will fit together to form a closed surface. Euclid found this problem difficult enough to be placed near the end of the *Elements*, and few of his readers ever mastered his solution. A beautiful direct construction was given by Luca Pacioli, a friend of Leonardo da Vinci's, in his book *De divina proportione* (1509). Pacioli's construction uses three copies of the *golden rectangle*, with sides 1 and $(1 + \sqrt{5})/2$, interlocking as in Figure 2.2. The 12 vertices define 20 triangles such as ABC , and it suffices to show that these are equilateral, that is, $AB = 1$. This is a straightforward exercise in the Pythagorean theorem (Exercise 2.2.2).

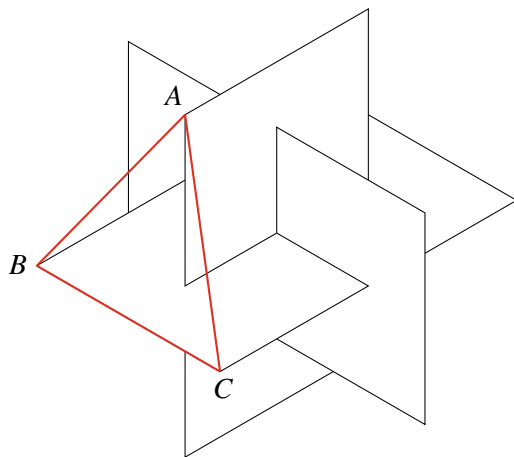


Figure 2.2: Pacioli's construction of the icosahedron

The regular polyhedra will make another important appearance in yet another 19th-century development, the theory of finite groups and Galois theory. See Chapter 14. Before the regular polyhedra made this triumphant comeback, they also took part in a famous fiasco: the Kepler (1596) theory of planetary distances. Kepler's theory is summarized by his famous diagram (Figure 2.3) of the five polyhedra, nested in such a way as to produce six spheres of radii proportional to the distances of the six planets then known. Unfortunately, although mathematics could not permit any more regular polyhedra, nature could permit more planets, and Kepler's theory was ruined when Uranus was discovered in 1781.

EXERCISES

The ratios between successive radii in Kepler's construction depend on what may be called the *inradius* and *circumradius* of each polyhedron—the radii of the spheres that touch it on the inside and the outside. It happens that the ratio

$$\frac{\text{circumradius}}{\text{inradius}}$$

is the same for the cube and the octahedron, and it is also the same for the dodecahedron and the icosahedron. This implies that the cube and octahedron can be exchanged in Kepler's construction, as can the dodecahedron and the icosahedron. Thus there are at least four different arrangements of the regular polyhedra that yield the same sequence of radii.

It is easy to see why the cube and the octahedron are interchangeable.

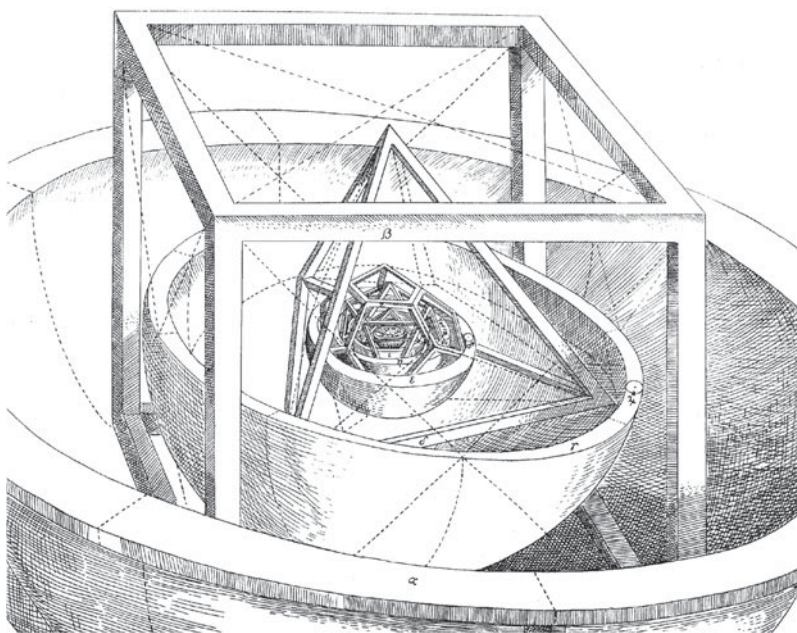


Figure 2.3: Kepler's diagram of the polyhedra

2.2.1 Show that $\frac{\text{circumradius}}{\text{inradius}} = \sqrt{3}$ for both the cube and the octahedron.

To compute circumradius/inradius for the icosahedron and the dodecahedron is quite difficult, and we will not pursue it further, other than verifying that Pacioli's construction gives a figure bounded by equilateral triangles.

2.2.2 Check Pacioli's construction: use the Pythagorean theorem to show that $AB = BC = CA$ in Figure 2.2. (It may help to use the additional fact that $\tau = (1 + \sqrt{5})/2$ satisfies $\tau^2 = \tau + 1$.)

2.3 Ruler and Compass Constructions

Greek geometers prided themselves on their logical purity; nevertheless, they were guided by intuition about physical space. One aspect of Greek geometry that was peculiarly influenced by physical considerations was the theory of constructions. Much of the elementary geometry of straight lines and circles can be viewed as the theory of constructions by ruler and compass. (By a "ruler" we mean simply a straightedge; it is not assumed to have any marks on it.) The very subject matter, lines and circles, reflects

the instruments used to draw them. And many of the elementary problems of geometry—for example, to bisect a line segment or angle, construct a perpendicular, or draw a circle through three given points—can be solved by ruler and compass constructions.

When coordinates are introduced, it is not hard to show that the points constructible from points P_1, \dots, P_n have coordinates in the set of numbers generated from the coordinates of P_1, \dots, P_n by the operations $+$, $-$, \times , \div , and $\sqrt{}$ (see Moise (1963) or the exercises to Section 5.3). Square roots arise, of course, because of the Pythagorean theorem: if points (a, b) and (c, d) have been constructed, then so has the distance $\sqrt{(c-a)^2 + (d-b)^2}$ between them (Section 1.5). Conversely, it is possible to construct \sqrt{l} for any given length l (Exercise 2.3.2).

Seen from this viewpoint, ruler and compass constructions look very special and unlikely to yield numbers such as $\sqrt[3]{2}$, for example. Just this number comes up in the classical Greek problem called *duplication of the cube*, since doubling the volume of a cube amounts to multiplying its side $\sqrt[3]{2}$. Other notorious problems were *trisection of the angle* and *squaring the circle*.¹ The latter problem was to construct a square equal in area to a given circle or to construct the number π , which amounts to the same thing. They sought ruler and compass solutions, though the possibility of a negative solution was admitted and solutions by less elementary means were tolerated. We will see some of these in the next sections.

The impossibility of solving these problems by ruler and compass constructions was not proved until the 19th century. For the duplication of the cube and trisection of the angle, impossibility was shown by Wantzel (1837). Wantzel seldom receives credit for settling these problems, which had baffled the best mathematicians for 2000 years, perhaps because his methods were superseded by the more powerful theory of algebraic numbers (see Chapter 16).

The impossibility of squaring the circle was proved by Lindemann (1882), in a very strong way. Not only is π undefinable by rational operations and square roots; it is also *transcendental*, that is, not the root of any polynomial equation with rational coefficients. Like Wantzel's work, this was a rare example of a major result proved by a minor mathematician. In

¹The term “squaring,” or its Latin equivalent “quadrature,” later became a general term for finding the area of curved regions, particularly in the 17th century, when calculus solved many such problems. Since ancient times the “squaring the circle” has been a popular phrase for trying to do the impossible.

Lindemann's case the explanation is perhaps that a major step had already been taken when Hermite (1873) proved the transcendence of e . Accessible proofs of both these results can be found in Klein (1924). Lindemann's subsequent career was mathematically undistinguished, even embarrassing. In response to skeptics who thought his success with π had been a fluke, he took aim at the most famous unsolved problem in mathematics, "Fermat's last theorem" (see Chapter 10 for the origin of this problem). His efforts fizzled out in a series of inconclusive papers, each one correcting an error in the one before. Fritsch (1984) has written an interesting biographical article on Lindemann.

One ruler and compass problem is still open: which regular n -gons are constructible? Gauss discovered in 1796 that the 17-gon is constructible and then showed that a regular n -gon is constructible if and only if $n = 2^m p_1 p_2 \cdots p_k$, where the p_i are distinct primes of the form $2^{2^h} + 1$. (This problem is also known as *circle division*, because it is equivalent to dividing the circumference of a circle, or the angle 2π , into n equal parts.) The proof of necessity was actually completed by Wantzel (1837). However, it is still not explicitly known what these primes are, or even whether there are infinitely many of them. The only ones known are for $h = 0, 1, 2, 3, 4$.

EXERCISES

Many of the constructions made by the Greeks are simplified by translating them into algebra, where it turns out that constructible lengths are those that can be built from known lengths by the operations of $+$, $-$, \times , \div , and $\sqrt{}$. It is therefore enough to know constructions for these five basic operations. Addition and subtraction are obvious, and the other operations are covered in the following exercises, together with an example in which algebra is a distinct advantage.

- 2.3.1** Show, using similar triangles, that if lengths l_1 and l_2 are constructible, then so are $l_1 l_2$ and l_1 / l_2 .
- 2.3.2** Use similar triangles to explain why \sqrt{l} is the length shown in Figure 2.4, and hence show that \sqrt{l} is constructible from l .

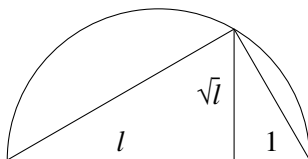


Figure 2.4: Square root construction

One of the finest ruler and compass constructions from ancient times is that of the regular pentagon, which includes, yet again, the golden ratio $\tau = (1 + \sqrt{5})/2$. Knowing (from the questions above) that this number is constructible, it becomes easy for us to construct the pentagon itself.

2.3.3 By finding some parallels and similar triangles in Figure 2.5, show that the diagonal x of the regular pentagon of side 1 satisfies $x/1 = 1/(x - 1)$.

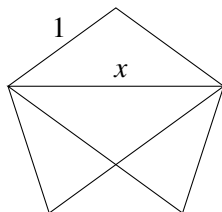


Figure 2.5: The regular pentagon

2.3.4 Deduce from Exercise 2.3.3 that the diagonal of the pentagon is $(1 + \sqrt{5})/2$ and hence that the regular pentagon is constructible.

2.4 Conic Sections

Conic sections are the curves obtained by cutting a circular cone by a plane: ellipses (including circles), parabolas, and hyperbolas (Figure 2.6, left to right). Today we know the conic sections better by their equations:

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1, \quad (\text{ellipse})$$

$$y = ax^2, \quad (\text{parabola})$$

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1. \quad (\text{hyperbola})$$

More generally, any second-degree equation represents a conic section or a pair of straight lines, a result that was proved by Descartes (1637).

The names “ellipse,” “parabola,” and “hyperbola” come from the Greek, meaning roughly “too little,” “alongside,” and “too much.” The ellipse arises by cutting with a plane that slopes too little (to make an infinite curve), the parabola from a plane parallel to one side of the cone, and the hyperbola from a plane that slopes too much to avoid hitting the other part of the cone, so it produces a curve with two branches.



Figure 2.6: Ellipse, parabola, hyperbola

The invention of conic sections is attributed to Menaechmus (fourth century BCE), a contemporary of Alexander the Great. Alexander is said to have asked Menaechmus for a crash course in geometry, but Menaechmus refused, saying, “There is no royal road to geometry.” Menaechmus used conic sections to give a very simple solution to the problem of duplicating the cube. In algebraic notation, this can be described as finding the intersection of the parabola $y = \frac{1}{2}x^2$ with the hyperbola $xy = 1$. This yields

$$x\frac{1}{2}x^2 = 1 \quad \text{or} \quad x^3 = 2.$$

The theory and practice of conic sections finally came together when Kepler (1609) found the orbits of the planets to be ellipses, and Newton (1687) explained this fact by his law of gravitation. This wonderful vindication of the theory of conic sections has often been seen as basic research receiving its long overdue reward, but perhaps one can also see it as a rebuke to Greek disdain for applications. As for Kepler himself . . . to the end of his days he was proudest of his theory explaining the distances of the planets in terms of the five regular polyhedra (Section 2.2).

EXERCISES

A key feature of the ellipse for both geometry and astronomy is a point called the *focus*. The term is the Latin word for fireplace, and it was introduced by Kepler. The ellipse actually has two foci, and they have the geometric property that the sum of the distances from the foci F_1 , F_2 to any point P on the ellipse is constant.

2.4.1 This property gives a way to draw an ellipse using two pins and piece of string. Explain how.

2.4.2 By introducing suitable coordinate axes, show that a curve with the above “constant sum” property indeed has an equation of the form

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1.$$

(It is a good idea to start with the two square root terms, representing the distances F_1P and F_2P , on opposite sides of the equation.) Show also that *any* equation of this form is obtainable by suitable choice of F_1 , F_2 , and $F_1P + F_2P$.

Another interesting property of the lines from the foci to a point P on the ellipse is that they make equal angles with the tangent at P . It follows that a light ray from F_1 to P is reflected through F_2 . A simple proof of this can be based on the *shortest-path property of reflection*, shown in Figure 2.7 and discovered by the Greek scientist Heron around 100 CE.

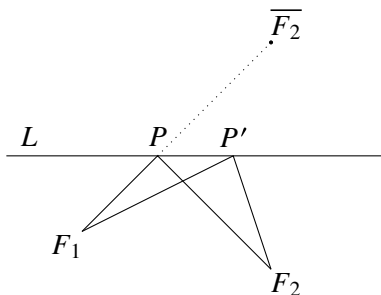


Figure 2.7: The shortest-path property

Shortest-path property. The path F_1PF_2 of reflection in the line L from F_1 to F_2 is shorter than any other path $F_1P'F_2$ from F_1 to L to F_2 .

2.4.3 Prove the shortest-path property, by considering the two paths $F_1P\overline{F_2}$ and $F_1P'F_2$, where $\overline{F_2}$ is the reflection of the point F_2 in the line L .

Thus to prove that the lines F_1P and F_2P make equal angles with the tangent, it is enough to show that F_1PF_2 is shorter than $F_1P'F_2$ for any other point P' on the tangent at P .

2.4.4 Prove this, using the fact that F_1PF_2 has the same length for all points P on the ellipse.

Kepler's great discovery was that the focus is also significant in astronomy. One focus is the point occupied by the sun as the planet moves along its ellipse.

2.5 Higher-Degree Curves

The Greeks lacked a systematic theory of higher-degree curves, because they lacked a systematic algebra. They could find what amounted to cartesian equations (in words) of individual curves—"symptoms," as they called them; see van der Waerden (1954), p. 241—but they did not consider equations in general or notice any of their properties relevant to the study of curves, for example, the degree. Nevertheless, they studied many interesting special curves, which Descartes and his followers cut their teeth on when algebraic geometry finally emerged in the 17th century. An excellent and well-illustrated account of these early investigations may be found in Brieskorn and Knörrer (1981), Chapter 1.

In this section we must confine ourselves to brief remarks on a few examples.

The Cissoid of Diocles (around 100 BCE)

This curve is defined using an auxiliary circle, which for convenience we take to be the unit circle, and vertical lines through x and $-x$. It consists of all the points P seen in Figure 2.8.

The portion shown in red results from varying x between 0 and 1. It is a cubic curve with cartesian equation

$$y^2(1+x) = (1-x)^3.$$

This equation shows that if (x, y) is a point on the curve, then so is $(x, -y)$. Hence one gets the complete picture of it by reflecting the portion shown in Figure 2.8 in the x -axis. The result is a sharp point at R , a *cusp*, a phenomenon that first arises with cubic curves. Diocles showed that the cissoid could be used to duplicate the cube, which is plausible (though still not obvious!) once one knows that this curve is cubic.

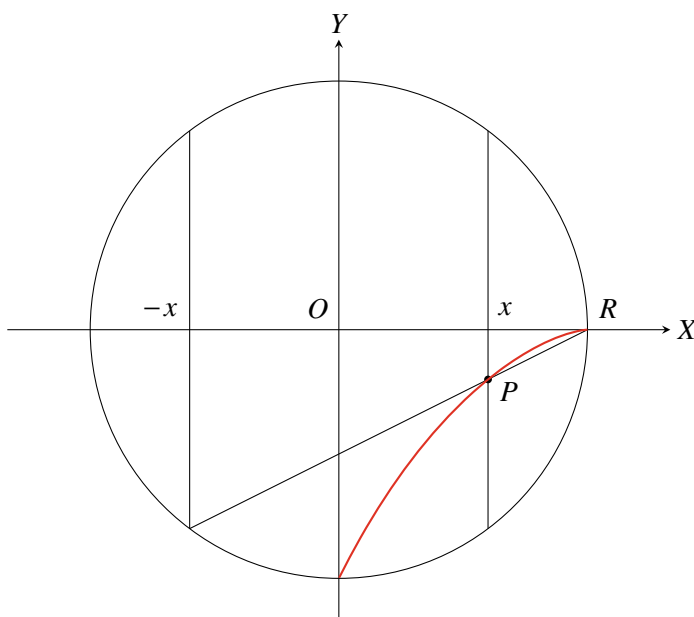


Figure 2.8: Construction of the cissoid

The Spiric Sections of Perseus (around 150 BCE)

Apart from the sphere, cylinder, and cone—whose sections are all conic sections—one of the few surfaces studied by the Greeks was the *torus*. This surface, generated by rotating a circle about an axis outside the circle, but in the same plane, was called a *spira* by the Greeks—hence the name spiric sections for the sections by planes parallel to the axis. These sections, which were first studied by Perseus, have four qualitatively distinct forms (see Figure 2.9).

These forms—convex ovals, “squeezed” ovals, the figure 8, and pairs of ovals—were rediscovered in the 17th century when analytic geometers looked at curves of degree 4, of which the spiric sections are examples. For suitable choice of torus, the figure 8 curve becomes the *lemniscate of Bernoulli* and the convex ovals become *Cassini ovals*. Cassini (1625–1712) was a distinguished astronomer but an opponent of Newton’s theory of gravitation. He rejected Kepler’s ellipses and instead proposed Cassini ovals as orbits for the planets.

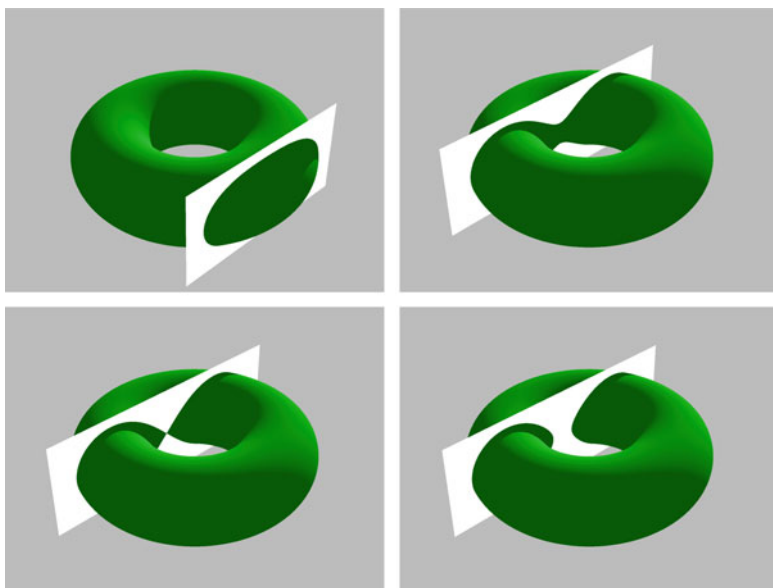


Figure 2.9: Spiric sections

The Epicycles of Ptolemy (140 CE)

These curves are known from a famous astronomical work, the *Almagest* of Claudius Ptolemy. Ptolemy himself attributes the idea to Apollonius. It seems almost certain that this is the Apollonius who mastered conic sections, which is ironic, because epicycles were his candidates for the planetary orbits, destined to be defeated by those very same conic sections.

An epicycle, in its simplest form, is the path traced by a point on a circle that rolls on another circle (Figure 2.10). More complicated epicycles can be defined by having a third circle roll on the second, and so on. The Greeks introduced these curves to try to reconcile the complicated movements of the planets, relative to the fixed stars, with a geometry based on the circle. In principle, this is possible! Lagrange (1772) showed that *any* motion along the celestial equator can be approximated arbitrarily closely by epicyclic motion, and a more modern version of the result may be found in Sternberg (1969). But Ptolemy's mistake was to accept the apparent complexity of the motions of the planets as actual in the first place. As we now know, the motion becomes simple when one considers motion relative to the sun rather than to the earth and allows orbits to be ellipses.

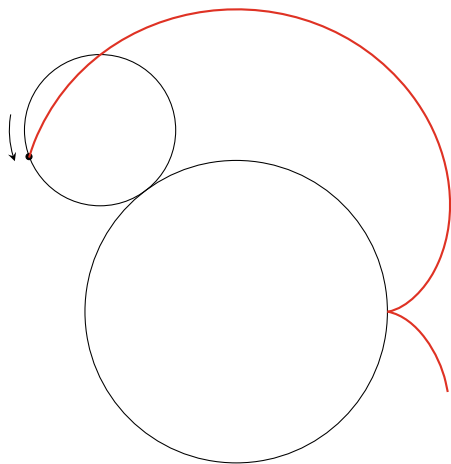


Figure 2.10: Generating an epicycle

Epicycles still have a role to play in engineering, and their mathematical properties are interesting. Some of them are closed curves and turn out to be algebraic, that is, of the form $p(x, y) = 0$ for a polynomial p . Others, such as those that result from rolling circles whose radii have an irrational ratio, lie densely in a certain region of the plane and hence cannot be algebraic; an algebraic curve $p(x, y) = 0$ can meet a straight line $y = mx + c$ in only a finite number of points, corresponding to roots of the polynomial equation $p(x, mx + c) = 0$, and the dense epicycles meet some lines infinitely often.

An obvious relative of the epicycles is the *cycloid*, the curve traced by a point on a circle that rolls on a straight line. The cycloid does not seem to have been studied by the Greeks, but it became a favorite of 17th-century mathematicians. As we will see in Chapter 13, spectacular properties of the cycloid were revealed by the methods of calculus.

EXERCISES

The equation of the cissoid is derivable as follows.

2.5.1 Using X and Y for the horizontal and vertical coordinates, show that the straight line RP in Figure 2.8 has equation

$$Y = \frac{\sqrt{1-x^2}}{1+x}(X-1).$$

2.5.2 Deduce the equation of the cissoid from Exercise 2.5.1.

The simplest epicyclic curve is the *cardioid* (“heart-shape”), which results from a circle rolling on a fixed circle of the same size.

2.5.3 Sketch a picture of the cardioid, confirming that it is heart-shaped (sort of).

2.5.4 Show that if both circles have radius 1, and we follow the point on the rolling circle initially at $(1, 0)$, then the cardioid it traces out has parametric equations

$$x = 2 \cos \theta - \cos 2\theta,$$

$$y = 2 \sin \theta - \sin 2\theta.$$

The cardioid is an algebraic curve. Its cartesian equation may be hard to discover, but it is easy to verify, especially if one has a computer algebra system.

2.5.5 Check that the point (x, y) on the cardioid satisfies

$$(x^2 + y^2 - 1)^2 = 4((x - 1)^2 + y^2).$$



3

Greek Number Theory

PREVIEW

Number theory is the second large field of mathematics that comes to us from the Pythagoreans via Euclid. The Pythagorean theorem led mathematicians to the study of squares and sums of squares; Euclid drew attention to the *primes* by proving that there are infinitely many of them.

His investigations were based on the *Euclidean algorithm*, a method for finding the greatest common divisor of two natural numbers. Common divisors are the key to basic results about prime numbers, in particular *unique prime factorization*, which says that each natural number factors into primes in exactly one way.

Another discovery of the Pythagoreans, the irrationality of $\sqrt{2}$, has consequences for natural numbers. Since $\sqrt{2} \neq m/n$ for any natural numbers m, n , there is no integer solution of the equation $x^2 - 2y^2 = 0$. But there are integer solutions of $x^2 - 2y^2 = 1$, and in fact infinitely many of them. The same is true of the equation $x^2 - Ny^2 = 1$ for any nonsquare natural number N .

The latter equation, called *Pell's equation*, is perhaps second in fame only to the Pythagorean equation $x^2 + y^2 = z^2$, among equations for which integer solutions are sought. Equations for which integer or rational solutions are sought are called *Diophantine*, after Diophantus. The methods he used to solve quadratic and cubic Diophantine equations are still of interest. We study his method for cubics in this chapter, and take it up again in Chapter 10.

3.1 The Role of Number Theory

In Chapter 1 we saw that number theory has been part of mathematics for at least as long as geometry, and from a foundational point of view it may be more important. Despite this, number theory resists a systematic treatment like that undergone by elementary geometry in Euclid's *Elements*. At all stages in its development, number theory has had glaring gaps because of the intractability of elementary problems. Most of the really old unsolved problems in mathematics, in fact, are simple questions about the natural numbers $1, 2, 3, \dots$. The nonexistence of a general method for solving Diophantine equations (Section 1.3) and the problem of identifying the primes of the form $2^{2^h} + 1$ (Section 2.3) have been noted. Other unsolved number theory problems will come up in the sections below.

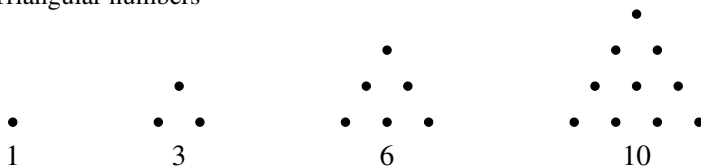
As a consequence, the role of number theory in the history of mathematics has been quite different from that of geometry. Geometry has played a stabilizing and unifying role, to the point of retarding further development at times and creating the popular impression that mathematics is a static subject. Number theory has been a spur to progress and change. Before 1800, only a handful of mathematicians contributed to advances in number theory, but they include some of the greats—Diophantus, Fermat, Euler, Lagrange, and Gauss. This book stresses advances in number theory that sprang from its connections with other parts of mathematics, particularly algebra and geometry, since these were the most significant for mathematics as a whole. For this reason we have no other chapter devoted purely to number theory, but there will be frequent excursions into number theory when we discuss algebra and what are called *elliptic curves*.

3.2 Polygonal, Prime, and Perfect Numbers

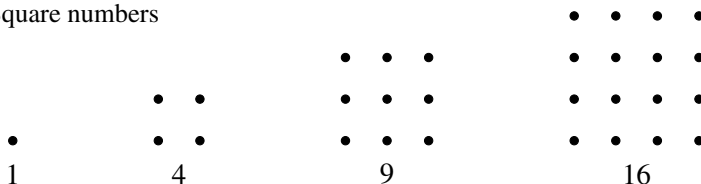
The *polygonal numbers*, which were studied by the Pythagoreans, result from a naive transfer of geometric ideas to number theory. From Figure 3.1 it is easy to calculate an expression for the m th n -gonal number as the sum of a certain arithmetic series (Exercise 3.2.3) and to show, for example, that a square is the sum of two triangular numbers. Apart from Diophantus's work, which contains impressive results on sums of squares, Greek results on polygonal numbers were of this elementary type.

On the whole, the Greeks seem to have been mistaken in attaching much importance to polygonal numbers. There are no major theorems about

Triangular numbers



Square numbers



Pentagonal numbers

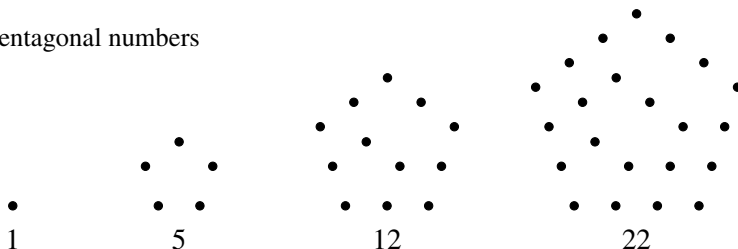


Figure 3.1: Polygonal numbers

them, except perhaps the following two. The first is the theorem conjectured by Bachet de Méziriac (1621) that every positive integer is the sum of four integer squares. This was proved by Lagrange (1770). A generalization, which Fermat (1670) stated without proof, is that every positive integer is the sum of n n -agonal numbers. This was proved by Cauchy (1813) but, somewhat disappointingly, all but four of the numbers can be 0 or 1. A short proof of Cauchy's theorem has been given by Nathanson (1987). The other remarkable theorem about polygonal numbers is the formula

$$\prod_{n=1}^{\infty} (1 - x^n) = 1 + \sum_{k=1}^{\infty} (-1)^k (x^{(3k^2-k)/2} + x^{(3k^2+k)/2})$$

proved by Euler (1750) and known as Euler's pentagonal number theorem, since the exponents $(3k^2 - k)/2$ are pentagonal numbers. For a proof see Hall (1967), p. 33.

The four-square theorem and the pentagonal number theorem were both absorbed around 1830 into Jacobi's theory of theta functions, a much larger theory. Theta functions are related to the *elliptic functions* that we study in Chapter 10.

The *prime numbers* were also considered within the geometric framework, as the numbers with no rectangular representation. A prime number, having no divisors apart from itself and 1, has only a “linear” representation. Of course this is merely a restatement of the definition of prime, and most theorems about prime numbers require much more powerful ideas; however, the Greeks did come up with one gem. This is the proof that there are infinitely many primes, in Book IX of Euclid's *Elements*.

Given any finite collection of primes p_1, p_2, \dots, p_n , we can find another by considering

$$p = p_1 p_2 \cdots p_n + 1.$$

This number is not divisible by p_1, p_2, \dots, p_n (each leaves remainder 1). Hence either p itself is a prime, and $p > p_1, p_2, \dots, p_n$, or else it has a prime divisor $\neq p_1, p_2, \dots, p_n$.

A *perfect number* is one that equals the sum of its divisors (including 1 but excluding itself). For example, $6 = 1 + 2 + 3$ is a perfect number, as is $28 = 1 + 2 + 4 + 7 + 14$. The concept goes back to the Pythagoreans, but only two notable theorems about perfect numbers are known. Euclid concludes Book IX of the *Elements* by proving that if $2^n - 1$ is prime, then $2^{n-1}(2^n - 1)$ is perfect (Exercise 3.2.5). These perfect numbers are of course even, and Euler (1849) (a posthumous publication) proved that every even perfect number is of Euclid's form. Euler's surprisingly simple proof may be found in Burton (1985), p. 504. It is unknown whether odd perfect numbers exist—this may be the oldest open problem in mathematics.

In view of Euler's theorem, all even perfect numbers arise from primes of the form $2^n - 1$. These are known as Mersenne primes, after Marin Mersenne (1588–1648), who first drew attention to the problem of finding primes of this form. It is not known whether there are infinitely many Mersenne primes, though larger and larger ones seem to be found quite regularly. In recent years each new world-record prime has been a Mersenne prime, giving a corresponding world-record perfect number.

EXERCISES

Infinitely many natural numbers are not sums of three (or fewer) squares. The smallest of them is 7, and it can be shown as follows that no number of the form $8n + 7$ is a sum of three squares.

3.2.1 Show that any square leaves remainder 0, 1, or 4 on division by 8.

3.2.2 Deduce that a sum of three squares leaves remainder 0, 1, 2, 3, 4, 5, or 6 on division by 8.

One reason polygonal numbers play only a small role in mathematics is that questions about them are basically questions about squares—hence the focus is on problems about squares.

3.2.3 Show that the k th pentagonal number is $(3k^2 - k)/2$.

3.2.4 Show that each square is the sum of two consecutive triangular numbers.

Euclid's theorem about perfect numbers depends on the prime divisor property, which will be proved in the next section. Assuming this for the moment, it follows that if $2^n - 1$ is a prime p , then the proper divisors of $2^{n-1}p$ (those unequal to $2^{n-1}p$ itself) are

$$1, 2, 2^2, \dots, 2^{n-1} \quad \text{and} \quad p, 2p, 2^2p, \dots, 2^{n-2}p.$$

3.2.5 Given that the divisors of $2^{n-1}p$ are those just listed, show that $2^{n-1}p$ is perfect when $p = 2^n - 1$ is prime.

3.3 The Euclidean Algorithm

This algorithm is named after Euclid because its earliest known appearance is in Book VII of the *Elements*. However, in the opinion of many historians (for example, Heath (1921), p. 399) the algorithm and some of its consequences were probably known earlier. At the very least, Euclid deserves credit for a masterly presentation of the fundamentals of number theory, based on this algorithm.

The Euclidean algorithm is used to find the greatest common divisor (gcd) of two positive integers a, b . The first step is to construct the pair (a_1, b_1) , where

$$\begin{aligned} a_1 &= \max(a, b) - \min(a, b), \\ b_1 &= \min(a, b), \end{aligned}$$

and then one simply repeats this operation of subtracting the smaller number from the larger. That is, if the pair constructed at step i is (a_i, b_i) , then the pair constructed at step $i + 1$ is

$$\begin{aligned} a_{i+1} &= \max(a_i, b_i) - \min(a_i, b_i), \\ b_{i+1} &= \min(a_i, b_i). \end{aligned}$$

The algorithm terminates at the first stage when $a_{i+1} = b_{i+1}$, and this common value is $\gcd(a, b)$. This is because taking differences preserves any common divisors; hence when $a_{i+1} = b_{i+1}$ we have

$$\gcd(a, b) = \gcd(a_1, b_1) = \cdots = \gcd(a_{i+1}, b_{i+1}) = a_{i+1} = b_{i+1}.$$

The sheer simplicity of the algorithm makes it easy to draw some important consequences. Euclid of course did not use our notation, but nevertheless he had results close to the following.

1. If $\gcd(a, b) = 1$, then there are integers m, n such that $ma + nb = 1$.

The equations

$$\begin{aligned} a_1 &= \max(a, b) - \min(a, b), \\ b_1 &= \min(a, b), \\ &\vdots \\ a_{i+1} &= \max(a_i, b_i) - \min(a_i, b_i), \\ b_{i+1} &= \min(a_i, b_i) \end{aligned}$$

show first that a_1, b_1 are integral linear combinations, $ma + nb$, of a and b , hence so are a_2, b_2 , hence so are a_3, b_3, \dots , and finally this is true of $a_{i+1} = b_{i+1}$. But $a_{i+1} = b_{i+1} = 1$, since $\gcd(a, b) = 1$; hence $1 = ma + nb$ for some integers m, n .

2. If p is a prime number that divides ab , then p divides a or b (the *prime divisor property*).

To see this, suppose p does *not* divide a . Then, since p has no other divisors except 1, we have $\gcd(p, a) = 1$. Hence by the previous result we get integers m, n such that

$$ma + np = 1.$$

Multiplying each side by b gives

$$mab + nbp = b.$$

By hypothesis, p divides ab ; hence p divides *both* terms on the left-hand side, and therefore p divides the right-hand side b .

3. Each positive integer has a unique factorization into primes (the *fundamental theorem of arithmetic*).

Suppose on the contrary that some integer n has two different prime factorizations:

$$n = p_1 p_2 \cdots p_j = q_1 q_2 \cdots q_k.$$

By removing common factors, if necessary, we can assume that there is a p_i that is not among the q 's. But this contradicts the previous result, because p_i divides $n = q_1 q_2 \cdots q_k$, yet it does not divide any of q_1, q_2, \dots, q_k individually, since these are prime numbers $\neq p_i$.

Induction

In this and the previous section we have glossed over an important point that Euclid was aware of but mentioned only briefly—the principle that *an infinite decreasing sequence of positive integers is impossible*. In the present section this *infinite descent* principle guarantees termination of the Euclidean algorithm, necessarily with the number $\gcd(a, b)$, for any pair of positive integers a, b . This is because the repeated subtraction process produces steadily decreasing numbers.

In the previous section infinite descent played a hidden role in Euclid's proof that there are infinitely many prime numbers: namely, in the assumption that *some* prime number divides $p_1 p_2 \cdots p_n + 1$. In Proposition 31 of Book VII of his *Elements*, Euclid proves existence of a prime divisor of any number N by repeatedly splitting N into smaller factors. If this process does not arrive at a prime factor then we get an infinite sequence of positive integers, each smaller than the one before. As Euclid says, this is "impossible in numbers."

Today, the impossibility of infinite descent is one way of stating *mathematical induction* (also known as *complete induction*), a method of proof that reflects the nature of positive integers as numbers that arise from 1 by repeatedly adding 1. On the one hand, this property implies that we arrive at 1 from any positive integer by stepping downward only finitely often. On the other hand, it implies that any positive integer can be reached from 1 by finitely often adding 1. In particular, a property P can be proved to hold for all positive integers by proving

1. P holds for the number 1 (the *base step*),
2. If P holds for n , then P holds for $n + 1$ (the *induction step*).

“Base step, induction step” is often considered the standard form of *proof by induction*, but it is perfectly fair to say that proofs by infinite descent, such as Euclid’s, are also proofs by induction.

Moreover, it is not generally appreciated that number theory needs induction as much as Euclid needed the parallel axiom in his geometry. The first to appreciate this fact was Grassmann (1861), who showed that all the basic algebraic properties of positive integers, such as $a + b = b + a$ and $ab = ba$, can be proved by induction. Even then, Grassmann’s breakthrough was buried in a school textbook, and not brought into general mathematical consciousness until the 1880s, when Peano (1889) formulated an axiom system for arithmetic with an *induction axiom* at its core. This system, called *Peano arithmetic* or PA, is an important part of the foundations of mathematics, as we will see in Chapter 17.

EXERCISES

We can now fill the gap in the proof of Euclid’s theorem on perfect numbers (previous exercise set), using the prime divisor property.

3.3.1 Use the prime divisor property to show that the proper divisors of $2^{n-1}p$, for any odd prime p , are $1, 2, 2^2, \dots, 2^{n-1}$ and $p, 2p, 2^2p, \dots, 2^{n-2}p$.

The result that if $\gcd(a, b) = 1$ then $1 = ma + nb$ for some integers m and n is a special case of the following way to represent the gcd.

3.3.2 Show that, for any integers a and b , there are integers m and n such that $\gcd(a, b) = ma + nb$.

This in turn gives a general way to find integer solutions of linear equations.

3.3.3 Deduce from Exercise 3.3.2 that the equation $ax + by = c$ with integer coefficients a, b , and c has an integer solution x, y if $\gcd(a, b)$ divides c .

The converse of this result is also valid, as one discovers when considering a *necessary* condition for $ax + by = c$ to have an integer solution.

3.3.4 The equation $12x + 15y = 1$ has no integer solution. Why?

3.3.5 (Solution of linear Diophantine equations) Give a test to decide, for any given integers a, b, c , whether there are integers x, y such that

$$ax + by = c.$$

3.4 Pell's Equation

The Diophantine equation $x^2 - Ny^2 = 1$, where N is a nonsquare integer, is known as Pell's equation because Euler mistakenly attributed a solution of it to the 17th-century English mathematician Pell (it should have been attributed to Brouncker). Pell's equation is probably the best-known Diophantine equation after the equation $a^2 + b^2 = c^2$ for Pythagorean triples, and in some ways it is more important. Solving Pell's equation is the main step in the solution of the general quadratic Diophantine equation in two variables (see, for example, Gelfond (1961)), and also a key tool in proving the theorem of Matiyasevich mentioned in Section 1.3 that there is no algorithm for solving all Diophantine equations (see, for example, Davis (1973) or Jones and Matiyasevich (1991)). In view of this, it is fitting that Pell's equation should make its first appearance in Greek mathematics, and it is impressive to see how well the Greeks understood it.

The simplest instance of Pell's equation,

$$x^2 - 2y^2 = 1,$$

was studied by the Pythagoreans in connection with $\sqrt{2}$. If x, y are large solutions to this equation, then $x/y \approx \sqrt{2}$, and the Pythagoreans found they could generate larger and larger solutions by the recurrence relations

$$x_{n+1} = x_n + 2y_n,$$

$$y_{n+1} = x_n + y_n.$$

A short calculation shows that

$$x_{n+1}^2 - 2y_{n+1}^2 = -(x_n^2 - 2y_n^2),$$

so if (x_n, y_n) satisfies $x^2 - 2y^2 = \pm 1$, then (x_{n+1}, y_{n+1}) satisfies $x^2 - 2y^2 = \mp 1$. Starting with the trivial solution $(x_0, y_0) = (1, 0)$ of $x^2 - 2y^2 = 1$, we get successively larger solutions $(x_2, y_2), (x_4, y_4), \dots$ of $x^2 - 2y^2 = 1$. (The pairs (x_n, y_n) were known as *side and diagonal numbers* because the ratio y_n/x_n tends to that of the side and diagonal in a square.)

But how might these recurrence relations have been discovered in the first place? Van der Waerden (1976) and Fowler (1980, 1982) suggest that the key is the Euclidean algorithm applied to line segments, an operation the Greeks called *anthyphairesis*. Given any two lengths a, b , one can define the sequence $(a_1, b_1), (a_2, b_2), \dots$, as in Section 3.2, by repeated subtraction of the smaller length from the larger. If a, b are integer multiples

of some unit, then the process terminates as in Section 3.3, but if b/a is irrational, it continues forever.

We can well imagine the Pythagoreans would have applied anthyphaire-sis to $a = 1$, $b = \sqrt{2}$. Here is what happens. If a, b are sides of a rectangle, each subtraction of the smaller number from the larger is represented by cutting off the square on the shorter side (Figure 3.2). We notice that the rectangle remaining after step 2, with sides $\sqrt{2} - 1$ and $2 - \sqrt{2} = \sqrt{2}(\sqrt{2} - 1)$, is the same shape as the original, though the long side is now vertical instead of horizontal. It follows that similar steps will recur forever—which is another proof that $\sqrt{2}$ is irrational, incidentally.

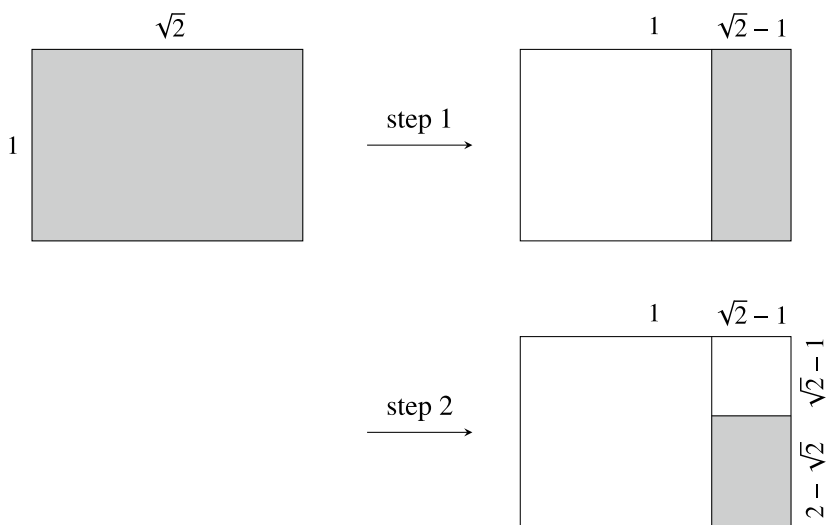


Figure 3.2: The Euclidean algorithm on $\sqrt{2}$ and 1

Now, however, we are interested in the relation between successive similar rectangles. If we let the long and short sides of successive similar rectangles be x_{n+1}, y_{n+1} and x_n, y_n , we can derive recurrence relations for x_{n+1}, y_{n+1} from Figure 3.3:

$$x_{n+1} = x_n + 2y_n,$$

$$y_{n+1} = x_n + y_n.$$

Exactly the relations of the Pythagoreans! The difference is that our x_n, y_n are not integers, and they satisfy $x^2 - 2y^2 = 0$, not $x^2 - 2y^2 = 1$.

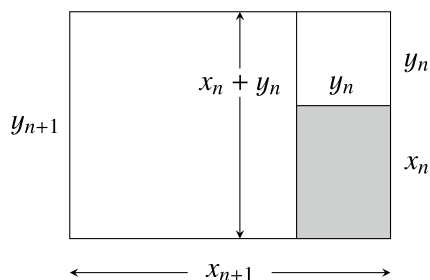


Figure 3.3: The recurrence relation

Nevertheless, one feels that Figure 3.3 gives the most natural interpretation of these relations. The discovery that the same relations generate solutions of $x^2 - 2y^2 = 1$ possibly arose from wishing that the Euclidean algorithm terminated with $x_1 = y_1 = 1$. If the Pythagoreans started with $x_1 = y_1 = 1$ and applied the recurrence relations, then they may well have found that (x_n, y_n) satisfies $x^2 - 2y^2 = (-1)^n$, as we did earlier.

Many other instances of the Pell equation $x^2 - Ny^2 = 1$ occur in Greek mathematics. In the seventh century CE the Indian mathematician Brahmagupta gave a procedure for generating larger solutions of $x^2 - Ny^2 = 1$ from known solutions. But *existence* of a solution, for any non-square N , was rigorously proved only in 1768 by Lagrange. The later European work on Pell's equation, which began in the 17th century with Brouncker and others, was based on the *continued fraction* for \sqrt{N} , though this amounts to the same thing as anthypharesis (see exercises). A short but detailed history of Pell's equation is in Dickson (1920), pp. 341–400.

An interesting aspect of the theory is the very irregular relationship between N and the number of steps before a rectangle proportional to the original recurs. If the number of steps is large, the smallest nontrivial solution of $x^2 - Ny^2 = 1$ is enormous. A famous example is what is called the *cattle problem* of Archimedes (287–212 BCE), which leads to the equation

$$x^2 - 4729494y^2 = 1.$$

Its smallest solution was found by Krummbiegel and Amthor (1880) to have 206,545 digits!

A recent paper on the cattle problem, Lenstra (2002), gives a strikingly condensed form of solution: “for the first time in history, *all* infinitely many solutions to the cattle problem are displayed in a handy little table.”

EXERCISES

The continued fraction of a real number $\alpha > 0$ is written

$$\alpha = n_1 + \frac{1}{n_2 + \frac{1}{n_3 + \frac{1}{n_4 + \frac{1}{\ddots}}}}$$

where $n_1, n_2, n_3, n_4, \dots$ are integers obtained by the following algorithm. Let

n_1 = integer part of α .

Then $\alpha - n_1 < 1$ and $\alpha_1 = 1/(\alpha - n_1) > 1$, so we can take

n_2 = integer part of α_1 .

Then $\alpha_1 - n_2 < 1$ and $\alpha_2 = 1/(\alpha_1 - n_2) > 1$, so we can take

n_3 = integer part of α_2 , and so on.

3.4.1 Apply the above algorithm to the number $\alpha = 157/68$, and hence show that

$$\frac{157}{68} = 2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{5}}}$$

You may notice that what happens is essentially the Euclidean algorithm applied to the pair $(157, 68)$, except that repeated operations of subtraction are replaced by division with remainder. The integers 2, 3, 4, 5 are the successive quotients obtained in these divisions: 157 divided by 68 gives quotient 2 and remainder 21, 68 divided by 21 gives quotient 3 and remainder 5, and so on.

Thus the Euclidean algorithm on integers a, b yields results that may be encoded by the (finite) continued fraction for a/b . This idea was introduced by Euler, and it became the preferred approach to the Euclidean algorithm for some mathematicians. Gauss (1801), in particular, always speaks of the Euclidean algorithm as the “continued fraction algorithm.”

The Euclidean algorithm on a pair $(\alpha, 1)$, where α is irrational, is indeed better known as the continued fraction algorithm.

3.4.2 Interpret the operations in the continued fraction algorithm—detaching the integer part and taking the reciprocal of the remainder—in terms of anthyphairesis.

3.4.3 Show that

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\ddots}}}}.$$

Exercise 3.4.3 implies that $\sqrt{2} + 1$ is the *periodic* continued fraction

$$2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\ddots}}}}.$$

3.4.4 Show that $\sqrt{3} + 1$ also has a periodic continued fraction, and hence derive the continued fraction for $\sqrt{3}$.

3.5 The Chord and Tangent Methods

In Section 1.3 we used a method of Diophantus to find all rational points on the circle. If $p(x, y) = 0$ is any quadratic equation in x and y with rational coefficients, and if the equation has one rational solution $x = r_1, y = s_1$, then we can find any rational solution by drawing a rational line $y = mx + c$ through the point r_1, s_1 and finding its other intersection with the curve $p(x, y) = 0$. The two intersections with the curve, $x = r_1, r_2$, say, are given by the roots r_1, r_2 of the equation

$$p(x, mx + c) = 0.$$

This means that $p(x, mx + c) = k(x - r_1)(x - r_2)$, and since all coefficients on the left-hand side are rational and r_1 is rational, then k and r_2 must also be rational. The y value when $x = r_2, y = s_2 = mr_2 + c$, is rational since m and c are; hence (r_2, s_2) is another rational point on $p(x, y) = 0$. Conversely, any line (or *chord*) through two rational points is rational, and hence all rational points are found in this way.

Now if $p(x, y) = 0$ is a curve of degree 3, its intersections with a line $y = mx + c$ are given by the roots of the cubic equation $p(x, mx + c) = 0$. If we know two rational points on the curve, then the line through them will

be rational, and its third intersection with the curve will also be rational, by an argument like the preceding one. This fact becomes more useful when one realizes that the two known rational points can be taken to *coincide*, in which case the line is the *tangent* through the known rational point. Thus from one rational solution we can generate another by the tangent construction, and from two we can construct a third by taking the chord between the two.

Diophantus found rational solutions to cubic equations in what seems to have been essentially this way. The surviving works of Diophantus reveal little of his methods, but a plausible reconstruction—an algebraic version of the tangent and chord constructions—has been given by Bashmakova (1981). Probably the first to understand Diophantus’s methods was Fermat, in the 17th century, and the first to give the tangent and chord interpretation was Newton (1670s).

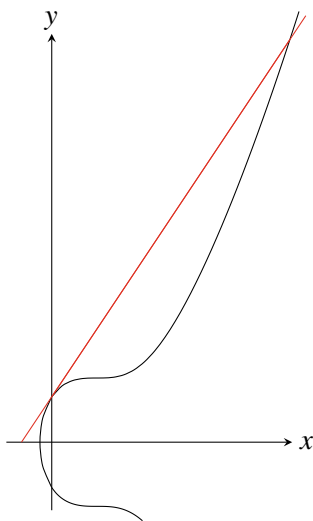


Figure 3.4: Cubic curve $y^2 = x^3 - 3x^2 + 3x + 1$ and tangent

In contrast to the quadratic case, we have no choice in the slope of the rational line for cubics. Thus it is unclear whether this method will give *all* rational points on a cubic. A remarkable theorem, conjectured by Poincaré (1901) and proved by Mordell (1922), says that all rational points can be generated by tangent and chord constructions applied to finitely many points. However, it is still not known whether there is an algorithm for finding a finite set of such rational generators on each cubic curve.

EXERCISES

3.5.1 Explain the solution $x = 21/4$, $y = 71/8$ to $x^3 - 3x^2 + 3x + 1 = y^2$ given by Diophantus (Heath (1910), p. 242) by constructing the tangent through the obvious rational point on this curve (Figure 3.4).

3.5.2 Rederive the following rational point construction of Viète (1593), p. 145. Given the rational point (a, b) on $x^3 - y^3 = a^3 - b^3$, show that the tangent at (a, b) is

$$y = \frac{a^2}{b^2}(x - a) + b,$$

and that the other intersection of the tangent with the curve is the rational point

$$x = a \frac{a^3 - 2b^3}{a^3 + b^3}, \quad y = b \frac{b^3 - 2a^3}{a^3 + b^3}.$$



4

Infinity in Greek Mathematics

PREVIEW

Perhaps the most interesting—and most modern—feature of Greek mathematics is its treatment of infinity. The Greeks feared infinity and tried to avoid it, but in doing so they laid the foundations for a rigorous treatment of infinite processes in 19th century calculus.

The most original contributions to the theory of infinity in ancient times were the *theory of proportions* and the *method of exhaustion*. Both were due to Eudoxus and expounded in Books V and XII of Euclid's *Elements*.

The theory of proportions develops the idea that a “quantity” λ (what we would now call a real number) can be known by its position among the rational numbers. That is, λ is known if we know the rational numbers less than λ and the rational numbers greater than λ . In a sense, the space less than λ can be “exhausted” by rational numbers.

The method of exhaustion generalizes this idea from quantities to regions of the plane or space. A region becomes known (in area or volume) when its position among known areas or volumes is known. For example, we know the area of a circle when we know the areas of the polygons inside it and the areas of polygons outside it; we know the volume of a pyramid when we know the volumes of stacks of prisms inside it and outside it.

Using this method, Euclid found that the volume of a tetrahedron equals $1/3$ of its base area times its height, and Archimedes found the area of a parabolic segment. Both of them relied on an infinite process that is fundamental to many calculations of area and volume: the summation of an infinite geometric series.

4.1 Fear of Infinity

Reasoning about infinity is one of the characteristic features of mathematics as well as its main source of conflict. In Chapter 1 we saw the conflict that arose from the discovery of irrationals, and in this chapter we will see that the Greeks rejected not only irrational numbers but infinite processes in general. In fact, until the late 19th century most mathematicians were reluctant to accept infinity as more than “potential.” The infinitude of a process, collection, or magnitude was understood as the possibility of its indefinite continuation, and no more—certainly not the possibility of completion. For example, the natural numbers $1, 2, 3, \dots$, can be accepted as a potential infinity—generated from 1 by the process of repeatedly adding 1—without accepting that there is a completed totality $\{1, 2, 3, \dots\}$. The same goes for any sequence x_1, x_2, x_3, \dots (of rational numbers, say), where x_{n+1} is obtained from x_n by a definite rule.

And yet a beguiling possibility arises when x_n tends to a *limit* x . If we already accept x —for geometric reasons, say—then it is tempting to view x as some kind of completion of the sequence x_1, x_2, x_3, \dots . It seems that the Greeks were afraid to draw such conclusions. According to tradition, they were frightened off by the paradoxes of Zeno, around 450 BCE.

We know of Zeno’s arguments only through Aristotle, who quotes them in his *Physics* in order to refute them, and it is not clear what Zeno himself wished to achieve. Was there, for example, a tendency toward speculation about infinity that he disapproved of? His arguments are so extreme they could almost be parodies of loose arguments about infinity he heard among his contemporaries. Consider his first paradox, the *dichotomy*:

There is no motion because that which is moved must arrive at the middle (of its course) before it arrives at the end.

Aristotle, *Physics*, Book VI, Ch. 9

The full argument presumably is that before getting anywhere one must first get half way, and before that a quarter of the way, and before that one eighth of the way, ad infinitum. The completion of this infinite sequence of steps no longer seems impossible to most mathematicians, since it represents nothing more than an infinite set of points within a finite interval. It must have frightened the Greeks though, because in all their proofs they were very careful to avoid completed infinities and limits.

The first mathematical processes we would recognize as infinite may be due to the Pythagoreans, for example, the recurrence relations

$$x_{n+1} = x_n + 2y_n,$$

$$y_{n+1} = x_n + y_n$$

for generating integer solutions of the equations $x^2 - 2y^2 = \pm 1$. We saw in Section 3.4 why it is likely that these relations arose from an attempt to understand $\sqrt{2}$, and it is easy for us to see that $x_n/y_n \rightarrow \sqrt{2}$ as $n \rightarrow \infty$.

However, it is unlikely that the Pythagoreans would have viewed $\sqrt{2}$ as a limit or seen the sequence as a meaningful object. The most we can say is that, by stating a recurrence, the Pythagoreans *implied* a sequence with limit $\sqrt{2}$. Only a much later generation of mathematicians could accept the infinite sequence as such and appreciate its ability to define a limit.

In a problem where we would reach a solution α by a limiting process, the Greeks would instead eliminate any solution *but* α . They would show that any number $<\alpha$ was too small, and any number $>\alpha$ was too large, to be the solution. We will study some examples of this style of proof below and see how it ultimately bore fruit in the foundations of mathematics. As a method of solving problems, however, it was sterile: how does one guess the number α in the first place? When mathematicians returned to problems of finding limits in the 17th century, they were in too much of a hurry for the rigorous methods of the Greeks. Their dubious, but efficient, methods of *infinitesimals* were criticized by the Zeno of the time, Bishop Berkeley, but little was done to meet his objections until much later. It was Dedekind, Weierstrass, and others in the 19th century who eventually restored Greek standards of rigor.

The story of rigor lost and rigor regained took an amazing turn when a previously unknown manuscript of Archimedes, *The Method*, was discovered in 1906. In it he reveals that his deepest results were found using dubious infinitary arguments, and only later proved rigorously. Because, as he says, “It is of course easier to supply the proof when we have previously acquired some knowledge of the questions by the method, than it is to find it without any previous knowledge.”

The importance of this statement goes beyond its revelation that infinity can be used to discover results that are not initially accessible to logic. Archimedes was probably the first mathematician candid enough to explain that there is a difference between the way theorems are discovered and the way they are proved.

4.2 Eudoxus's Theory of Proportions

The theory of proportions is credited to Eudoxus (around 400–350 BCE) and is expounded in Book V of Euclid's *Elements*. Its purpose is to let lengths (and other geometric quantities) be treated as precisely as numbers, while admitting only the use of rational numbers. We saw the motivation for this in Section 1.5: the Greeks could not accept irrational numbers, but they accepted irrational geometric quantities such as the diagonal of the unit square. To simplify the exposition of the theory, let us call lengths *rational* if they are rational multiples of a fixed length.

The idea of Eudoxus was to say that a length λ is determined by those rational lengths less than it and those greater than it. To be precise, he says $\lambda_1 = \lambda_2$ if any rational length $<\lambda_1$ is also $<\lambda_2$, and vice versa. Likewise $\lambda_1 < \lambda_2$ if there is a rational length $>\lambda_1$ but $<\lambda_2$. This definition uses the rationals to give an infinitely sharp notion of length while avoiding any overt use of infinity. Of course the infinite set of rational lengths $<\lambda$ is present in spirit, but Eudoxus avoids mentioning it by speaking of an arbitrary rational length $<\lambda$.

The theory of proportions was so successful that it delayed the development of a theory of real numbers for 2000 years. This was ironic, because the theory of proportions can be used to define irrational numbers just as well as lengths. It was understandable though, because the common irrational lengths, such as the diagonal of the unit square, arise from constructions that are intuitively clear and finite from the geometric point of view. Any *arithmetic* approach to $\sqrt{2}$, whether by sequences, decimals, or continued fractions, is infinite and therefore less intuitive. Until the 19th century this seemed a good reason for considering geometry to be a better foundation for mathematics than arithmetic. Then the problems of geometry came to a head, and mathematicians began to fear geometric intuition as much as they had previously feared infinity. There was a purge of geometric reasoning from the textbooks and industrious reconstruction of mathematics on the basis of numbers and sets of numbers. Set theory is discussed further in Chapter 17. Suffice to say, for the moment, that set theory depends on the acceptance of completed infinities.

The beauty of the theory of proportions was its adaptability to this new climate. Instead of rational lengths, take rational numbers. Instead of comparing existing irrational lengths by means of rational lengths, construct irrational numbers from scratch using sets of rationals! The length $\sqrt{2}$ is

determined by the two sets of positive rationals

$$L_{\sqrt{2}} = \{r : r^2 < 2\}, \quad U_{\sqrt{2}} = \{r : r^2 > 2\}.$$

Dedekind (1872) decided in effect to let $\sqrt{2}$ be this pair of sets! In general, let any partition of the positive rationals into sets L, U such that any member of L is less than any member of U be a positive real number. This idea, now known as a *Dedekind cut*, is more than just a twist of Eudoxus; it gives a complete and uniform construction of all real numbers, or points on the line, using just the rationals. In short, it is an explanation of the *continuous* in terms of the *discrete*, finally resolving the fundamental conflict in Greek mathematics. Dedekind was understandably pleased with his achievement. He wrote

The statement is so frequently made that the differential calculus deals with continuous magnitude, and yet an explanation of this continuity is nowhere given. . . . It then only remained to discover its true origin in the elements of arithmetic and thus at the same time secure a real definition of the essence of continuity. I succeeded Nov. 24 1858.

Dedekind (1872), p. 2

EXERCISES

There is only one Dedekind cut (L, U) corresponding to an irrational number α , but there are two cuts corresponding to a rational number a :

$$L = \{r : r \leq a\}, \quad U = \{r : r > a\}$$

and

$$L = \{r : r < a\}, \quad U = \{r : r \geq a\}.$$

To unify the theory of all reals we choose the latter cut, call it

$$L_a = \{r : r < a\}, \quad U_a = \{r : r \geq a\},$$

as the standard way to represent a rational a . We can then say, whether x is rational or irrational, that the lower set for x is

$$L_x = \{r : r < x\}.$$

Now we use lower sets to define $x+y$ and xy for positive reals x and y as follows:

$$L_{x+y} = \{r + s : r < x \text{ and } s < y, \text{ where } r, s \text{ are rational}\}$$

$$L_{xy} = \{rs : r < x \text{ and } s < y, \text{ where } r, s \text{ are rational}\}.$$

4.2.1 Show that these are valid definitions of $x + y$ and xy when x and y are rational.

The test of these definitions, as Dedekind realized, is that they allow rigorous proofs of results like $\sqrt{2}\sqrt{3} = \sqrt{6}$ that (in Dedekind's opinion) had never been rigorously proved before. Proofs using Dedekind's definitions are possible, but not trivial. Even to prove that $\sqrt{2}\sqrt{2} = 2$ one has to prove the next two results.

4.2.2 If $r^2 < 2$ and $s^2 < 2$, show that $rs < 2$.

4.2.3 If a rational $t < 2$, show that $t = rs$ for some rationals r, s with $r^2 < 2$, $s^2 < 2$. (Hint: Choose r with $t \leq r^2 < 2$.)

4.2.4 Why do Exercises 4.2.2 and 4.2.3 show that $\sqrt{2}\sqrt{2} = 2$?

4.2.5 Give a similar proof that $\sqrt{2}\sqrt{3} = \sqrt{6}$.

4.3 The Method of Exhaustion

The method of exhaustion, also credited to Eudoxus, is a generalization of his theory of proportions. Just as an irrational length is determined by the rational lengths on either side of it, more general unknown quantities become determined by arbitrarily close approximations using known figures. Examples given by Eudoxus (and expounded in Book XII of Euclid's *Elements*) are an approximation of the circle by inner and outer polygons (Figure 4.1) and an approximation of a tetrahedron by stacks of prisms (Figure 4.2, which shows the most obvious approximation, not the cunning one used by Euclid, which is shown in Figure 4.5). In both cases the approximating figures are known quantities, on the basis of the theory of proportions and the theorem that area of triangle = $1/2$ base \times height.

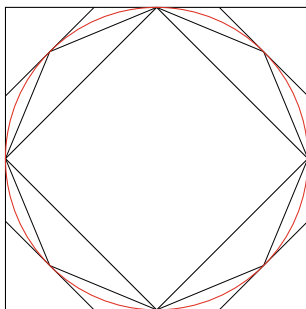


Figure 4.1: Approximating a circle

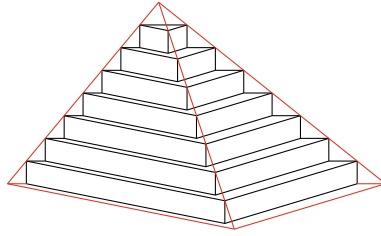


Figure 4.2: Approximating a tetrahedron

The polygonal approximations are used to show that the area of any circle is proportional to the square on its radius, as follows. Suppose $P_1 \subset P_2 \subset P_3 \subset \dots$ are the inner polygons and $Q_1 \supset Q_2 \supset Q_3 \supset \dots$ are the outer polygons. Each polygon is obtained from its predecessor by bisecting the arcs between its vertices, as shown in Figure 4.1. It can then be shown, by elementary geometry, that the area difference $Q_i - P_i$ can be made arbitrarily small, and hence P_i approximates the area C of the circle arbitrarily closely.

On the other hand, elementary geometry also shows that the area P_i is proportional to the square, R^2 , of the radius. Writing the area as $P_i(R)$ and using the theory of proportions to handle ratios of areas, we have

$$P_i(R) : P_i(R') = R^2 : R'^2. \quad (1)$$

Now let $C(R)$ denote the area of the circle of radius R , and suppose

$$C(R) : C(R') < R^2 : R'^2. \quad (2)$$

By choosing a P_i that approximates C sufficiently closely we also get

$$P_i(R) : P_i(R') < R^2 : R'^2,$$

which contradicts (1). Hence the $<$ sign in (2) is incorrect, and we can similarly show that $>$ is incorrect. Thus the only possibility is

$$C(R) : C(R') = R^2 : R'^2,$$

that is, the area of a circle is proportional to the square of its radius. That is, *the constant of proportionality π in the formula πR^2 for the area of the circle is independent of the radius R .*

Notice that “exhaustion” does not mean using an infinite sequence of steps to show that area is proportional to the square of the radius. Rather, one refutes any *disproportionality* in a *finite* number of steps (by going to a suitable P_i). This is typical of the way in which exhaustion arguments avoid mention of limits and infinity.

It is interesting that Euclid does *not* need the method of exhaustion in the theory of area for polygons. It can be done entirely by dissection arguments such as that showing area of triangle = $1/2$ base \times height (Figure 4.3). In fact, it was shown by Farkas Bolyai (1832a) that any polygons P , Q of equal area can be cut into polygonal pieces P_1, \dots, P_n and Q_1, \dots, Q_n such that P_i is congruent to Q_i . Thus we can *define* polygons to be equal in area if they possess dissections into such correspondingly congruent pieces.

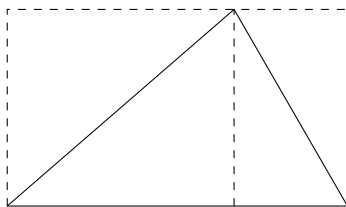


Figure 4.3: Area of a triangle

In Hilbert’s famous list of mathematical problems, Hilbert (1900a), the third was to decide whether an analogous definition was possible for polyhedra. Dehn (1900) showed that it was not; in fact, a tetrahedron and a cube of equal volume cannot be dissected into corresponding congruent polyhedral pieces. Hence infinite processes of some kind, such as the method of exhaustion, are needed to define equality of volume. A readable account of Dehn’s theorem and related results may be found in Boltyansky (1978).

EXERCISES

Another approach to the volume of the tetrahedron by exhaustion is in Euclid (see Heath (1925), Book XII, Proposition 4). He dissected the tetrahedron into two smaller tetrahedra and two prisms as shown in Figure 4.4, with vertices at the edge midpoints of the original tetrahedron. (There is a “front” prism, with triangles left and right, and a “back” prism, with triangles top and bottom.)

- 4.3.1** Show that the two prisms occupy more than half of the tetrahedron. (Hence, by iterating the construction in the smaller tetrahedra, the volume of the tetrahedron may be approximated arbitrarily closely by prisms.)

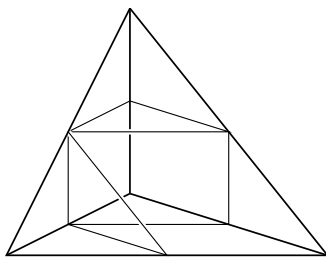


Figure 4.4: Euclid's dissection of the tetrahedron

4.3.2 Show that the volume of the two prisms in Figure 4.4 is $1/4$ base \times height (the base and height of the tetrahedron, that is).

By computing the volumes of the corresponding prisms in the smaller tetrahedra (Figure 4.5), and repeating, we find the volume of the original tetrahedron as a sum of a geometric series.

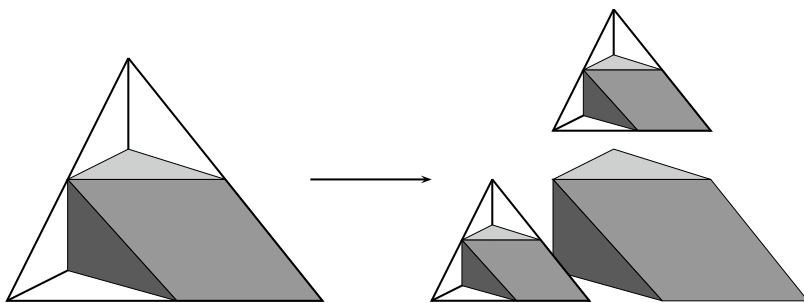


Figure 4.5: Repeated dissection of the tetrahedron

4.3.3 Show that the total volume of the prisms is

$$\left(\frac{1}{4} + \frac{1}{4^2} + \frac{1}{4^3} + \cdots \right) \text{base} \times \text{height} = 1/3 \text{ base} \times \text{height}.$$

In the next section we study a construction of Archimedes that is curiously similar to this one of Euclid. Each step cuts pieces out of the leftovers from the previous step and leads to a similar geometric series. While it is convenient for us to view the process as summing an infinite geometric series, both Euclid and Archimedes applied an exhaustion argument to finite (but arbitrarily long) geometric series.

4.4 The Area of a Parabolic Segment

The method of exhaustion was brought to full maturity by Archimedes (287–212 BCE). Among his most famous results are the volume and surface area of the sphere and the area of a parabolic segment. As mentioned in Section 4.1, Archimedes first discovered these results by nonrigorous methods, later confirming them by the method of exhaustion. Perhaps the most interesting and natural of his exhaustion proofs is the one for the area of the parabolic segment. The segment is exhausted by polygons similarly to Eudoxus' exhaustion of the circle, but the area is obtained outright and not merely in proportion to another figure.

To simplify the construction slightly we assume that the segment is cut off by a chord perpendicular to the axis of symmetry of the parabola. Archimedes divides the parabolic segment into triangles $\Delta_1, \Delta_2, \Delta_3, \dots$, as shown in Figure 4.6 (labeled by their subscripts). The middle vertex of each triangle lies on the parabola halfway between the other two (measured horizontally). These triangles clearly exhaust the parabolic segment, and so it remains to compute their area. Quite surprisingly, this turns into a geometric series.

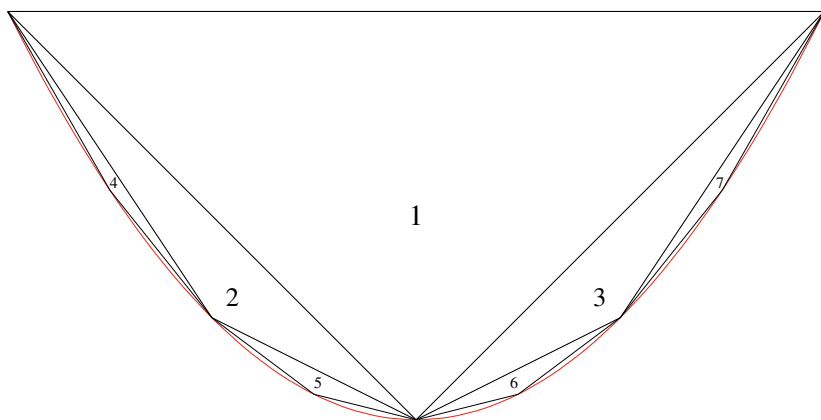


Figure 4.6: The parabolic segment

We indicate how this comes about by looking at Δ_3 (Figure 4.7).

Since $OP = \frac{1}{2}OX$, $PQ = \frac{1}{4}PS$ by definition of the parabola. On the other hand, $SR = \frac{1}{2}PS$, so $QR = \frac{1}{4}PS$. Now Δ_3 is the sum of the triangles RQZ and OQR , which have the same base RQ and height $OP = PX$, hence equal area. We have just seen that RQZ has half the base of SRZ and it

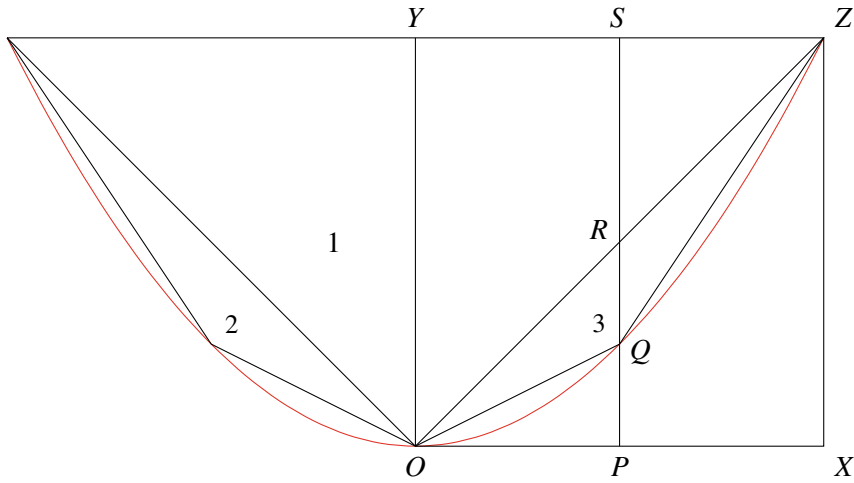


Figure 4.7: A triangle in the segment

has the same height; hence (calling figures equal when they have the same area)

$$\Delta_3 = SRZ = \frac{1}{4}OYZ = \frac{1}{8}\Delta_1.$$

By symmetry, $\Delta_2 = \Delta_3$, so $\Delta_2 + \Delta_3 = \frac{1}{4}\Delta_1$.

A similar argument shows that

$$\Delta_4 + \Delta_5 + \Delta_6 + \Delta_7 = \frac{1}{16}\Delta_1$$

and so on, each new chain of triangles having one-fourth the area of the previous chain. Consequently,

$$\begin{aligned} \text{area of parabolic segment} &= \Delta_1 \left(1 + \frac{1}{4} + \left(\frac{1}{4}\right)^2 + \cdots \right) \\ &= \frac{4}{3}\Delta_1. \end{aligned}$$

Of course, Archimedes does not use the infinite series but uses exhaustion, showing that any area $< \frac{4}{3}\Delta_1$ can be exceeded by taking sufficiently many of the triangles Δ_i . The sum of the *finite* geometric series needed for this was known from Euclid's *Elements*, Book IX, where Euclid used it for the theorem about perfect numbers (Section 3.2).

EXERCISES

Archimedes' method of approximation by triangles was a brilliant success on the parabolic segment, but not suited to many other curves. A more generally useful method is approximation by rectangles, probably known to you from calculus. The area of a parabolic segment can also be computed in this way, though less gracefully, and indeed Archimedes did this too. We look at other curved areas that can be evaluated by rectangle approximation in Section 8.2.

Probably the simplest area that *cannot* be found by this method is the area under the hyperbola $y = 1/x$, from $x = 1$ to $x = t$. This is because the area in question is $\log t$, and the logarithm function cannot be defined by elementary means. But if instead one takes the area to be $\log t$ by *definition*, then it is possible to derive the basic *property* of the logarithm—

$$\log ab = \log a + \log b$$

—and by means Archimedes would have understood.

4.4.1 Suppose we approximate the area $\log a$ under $y = 1/x$ from 1 to a by n rectangles of equal width, as shown in Figure 4.8.

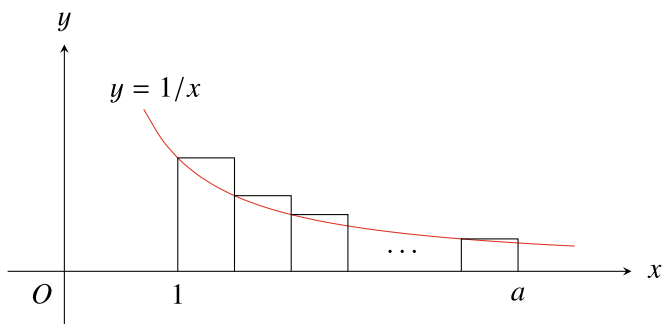


Figure 4.8: Rectangle approximation to $\log a$

Show that the corresponding approximation to the area under $y = 1/x$ from b to ab by n rectangles has exactly the same area. (In fact, corresponding rectangles have equal area.)

4.4.2 Deduce from Exercise 4.4.1, by the method of exhaustion, that the area under $y = 1/x$ from 1 to a equals the area under $y = 1/x$ from b to ab .

4.4.3 Deduce from Exercise 4.4.2, and the above definition of \log , that

$$\log ab = \log a + \log b.$$



5

Polynomial Equations

PREVIEW

The first phase in the history of algebra was the search for solutions of polynomial equations. The “degree of difficulty” of an equation corresponds rather well to the degree of the corresponding polynomial.

Linear equations are easily solved, and 2000 years ago the Chinese were even able to solve n linear equations in n unknowns by the method we now call “Gaussian elimination.”

Quadratic equations are harder to solve, because they generally require the square root operation. But the solution—essentially the same as that taught in high schools today—was discovered independently in many cultures more than 1000 years ago.

The first really hard case is the cubic equation, whose solution requires both square roots and cube roots. Its discovery by Italian mathematicians in the early 16th century was a decisive breakthrough, and equations quickly became the language of virtually all mathematics then known (See, for example, algebraic geometry in Chapter 6 and calculus in Chapter 8.)

Despite this breakthrough, the problem of polynomial equations was far from solved. The obstacle is the *quintic* equation—the general equation of degree 5. In the 1820s it finally became clear that the quintic equation is *not* solvable in the sense that equations of lower degree are solvable. But explaining why this is so requires a new, and more abstract, concept of algebra (see Chapter 14).

A rather special, but important, thread in the history of algebra is the *binomial theorem*. Here we sketch its origins and how they led to early developments in combinatorics, probability, and number theory.

5.1 Algebra

The word “algebra” comes from the Arabic word *al-jabr* meaning “restoring.” It passed into mathematics through the book *Al-jabr w'al mûqabala* (Science of restoring and opposition) of al-Khwārizmī in 830 CE, a work on the solution of equations. In this context, “restoring” meant adding equal terms to both sides and “opposition” meant setting the two sides equal. For centuries, *al-jabr* more commonly meant the resetting of broken bones, and the surgical meaning accompanied the mathematical one when “*al-jabr*” became “algebra” in Spanish, Italian, and English. Even today the surgical meaning is included in the *Oxford English Dictionary*. Al-Khwārizmī’s own name has given us the word “algorithm,” so his work has had a lasting impact on mathematics, even though its content was quite elementary.

His algebra went no further than the solution of quadratic equations, which had already been understood by the Babylonians, presented from the geometric viewpoint by Euclid, and reduced to a formula by Brahmagupta (628) (see Section 5.3). Brahmagupta’s work, the high point of Indian mathematics to that time, was more advanced than al-Khwārizmī’s in several respects—notation, admission of negative numbers, and the treatment of Diophantine equations—even though it predated al-Khwārizmī and was very likely known to him. Indian mathematics had spread to the Muslim world with the general promotion of culture by the eighth-century caliphs of Baghdad, and Muslim mathematicians acknowledged the Indian origin of certain ideas, such as decimal numerals. Why then did al-Khwārizmī’s work rather than Brahmagupta’s become the definitive “algebra”?

Perhaps the time was ripe for the idea of algebra to be cultivated, and the simple algebra of al-Khwārizmī served this purpose better than those of his more sophisticated predecessors. In Indian mathematics, algebra was inseparable from number theory. In Greek mathematics, algebra was hidden by geometry. Other possible sources of algebra, Babylonia and China, were lost or cut off from the West until it was too late for them to be influential. The concept of algebra that emerged from al-Khwārizmī—the theory of polynomial equations—lasted for 1000 years. Only in the 19th century did algebra grow beyond these bounds, and this was a time when most fields of mathematics were outgrowing their established habitats. For a detailed history of algebra, which emphasizes the tradition of solving equations, see Katz and Parshall (2014). For the new developments from the 19th century onward see Gray (2018).

The early algebraic methods were essentially geometric methods, as we will see in the case of quadratic equations in Section 5.3. Algebraic methods for solving equations became distinct from, and superior to, the geometric only with new manipulative techniques and efficient notation in the 16th century (Section 5.5). Algebra did not break away from geometry, however, but actually gave it a new lease on life, thanks to the development of algebraic geometry by Fermat and Descartes around 1630. This reunion of algebra and geometry at a higher level is discussed in Chapter 6.

The story of algebraic geometry unfolds along with the story of polynomial equations, becoming entwined with many other mathematical threads in the process. One we have already seen is Diophantus's chord and tangent method for finding rational solutions of equations (Section 3.5). Another relevant event, though not historically connected with Western mathematics, was the method of elimination developed by Chinese mathematicians between the early Christian era and the Middle Ages. Since this method concerns equations of the lowest degree, it is logical to discuss it first.

5.2 Linear Equations and Elimination

The Chinese discovered a method for solving linear equations in any number of unknowns during the Han dynasty (206 BCE–220 CE). It appears in the famous book *Jiuzhang suanshu* (Nine Chapters of Mathematical Art; see Shen et al. (1999)), which survives today in a third-century version with a commentary by Liu Hui. The method was essentially what we call *Gaussian elimination*, systematically eliminating terms in a system

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &= b_n \end{aligned}$$

by subtracting a suitable multiple of each equation from the one below it until a triangular system is obtained:

$$\begin{aligned} a'_{11}x_1 + a'_{12}x_2 + \cdots + a'_{1n}x_n &= b'_1 \\ a'_{22}x_2 + \cdots + a'_{2n}x_n &= b'_2 \\ &\vdots \\ a'_{nn}x_n &= b'_n \end{aligned}$$

then solving for x_n, x_{n-1}, \dots, x_1 in turn by successive substitutions. Such calculations were particularly well suited to a Chinese device called the counting board, which held the array of coefficients and allowed “row operations” like those we perform with matrices. For further details, see Li and Du (1987) or Martzloff (2006).

Around the 12th century, Chinese mathematicians found that elimination could be adapted to simultaneous polynomial equations in two or more variables. For example, one can eliminate y between the pair of equations

$$a_0(x)y^m + a_1(x)y^{m-1} + \cdots + a_m(x) = 0, \quad (1)$$

$$b_0(x)y^m + b_1(x)y^{m-1} + \cdots + b_m(x) = 0, \quad (2)$$

where the $a_i(x), b_j(x)$ are polynomials in x . The y^m term can be eliminated by forming the equation $b_0(x) \times (1) - a_0(x) \times (2)$, say,

$$c_0(x)y^{m-1} + c_1(x)y^{m-2} + \cdots + c_{m-1}(x) = 0. \quad (3)$$

We can form a second equation of degree $m-1$ in y by multiplying (3) by y , then again eliminating y^m between $(3) \times y$ and (1), giving, say,

$$d_0(x)y^{m-1} + d_1(x)y^{m-2} + \cdots + d_{m-1}(x) = 0. \quad (4)$$

The problem is now reduced to eliminating y between the equations (3) and (4), which are of lower degree in y than (1) and (2). Thus one can continue inductively until an equation in x alone is obtained. This method was extended to four variables in the work of Zhū Shijié (1303) entitled *Siyuan yujian* (Jade Mirror of Four Unknowns).

As we will see in Chapter 6, the two-variable polynomial problem arose in the West in the 17th century, in the context of finding intersections of curves. This led first to a rediscovery of the method of elimination for polynomials; only later was this method based on an understanding of linear equations (and *determinants*, see Chapter 16). The well-known Cramer’s rule for solving linear equations using determinants was named after its appearance in a book on algebraic curves, Cramer (1750).

EXERCISES

The first interesting case of elimination between two-variable polynomials occurs when the polynomials have degree 2. Geometrically, this amounts to finding the intersections of two conic sections.

5.2.1 Derive an equation that is linear in y from the two equations

$$\begin{aligned}x^2 + xy + y^2 &= 1, \\4x^2 + 3xy + 2y^2 &= 3,\end{aligned}$$

and hence show that $y = (1 - 2x^2)/x$.

5.2.2 Deduce that the intersections of the two curves in Exercise 5.2.1 occur where x satisfies $3x^4 - 4x^2 + 1 = 0$.

This example, where the two equations of degree 2 yield a single equation of degree 4 ($= 2 \times 2$), illustrates a general phenomenon where degrees are multiplied. We will observe other instances, and study it more deeply, as the book progresses.

The present example is not a typical equation of degree 4, since it is quadratic in $x^2 = z$. However, this makes it a lot easier to solve.

5.2.3 Solve $3z^2 - 4z + 1 = 0$ for $z = x^2$ by factorizing the left-hand side, and hence find four solutions for x .

Give geometric reasons why you would expect two curves of degree 2 to have up to four intersections. Could they have more than four?

The *Jade Mirror of Four Unknowns* does not go beyond four equations in four unknowns (hence the name). The idea is quite general, but it becomes hard to implement on the counting board when there are more than four unknowns. An amusing problem in three unknowns from the *Jade Mirror*, which does not require the full strength of the elimination method, is given in the exercises below.

5.2.4 Problem 2 in the *Jade Mirror* (see Hoe (1977), p. 135) is to find the side a of a right-angled triangle (a, b, c) such that

$$\begin{aligned}a^2 - (b + c - a) &= ab, \\b^2 + (a + c - b) &= bc.\end{aligned}$$

The *Jade Mirror* suggests choosing the unknowns $x = a$ and $y = b + c$. Using $a^2 = c^2 - b^2$, show that this implies

$$\begin{aligned}b &= (y - x^2/y)/2, \\c &= (y + x^2/y)/2.\end{aligned}$$

5.2.5 Deduce that the first two equations in Exercise 5.2.4 are equivalent, respectively, to

$$\begin{aligned}(-2 - x)y^2 + (2x + 2x^2)y + x^3 &= 0, \\(2 - x)y^2 + 2xy + x^3 &= 0.\end{aligned}$$

5.2.6 By subtracting one equation in Exercise 5.2.5 from the other, deduce that $y = x^2/2$. Substitute this back to obtain a quadratic equation for x , with solution $x = a = 4$. What are the values of b and c ?

5.3 Quadratic Equations

As early as 2000 BCE, the Babylonians could solve a pair of simultaneous equations of the form

$$x + y = p,$$

$$xy = q,$$

which are equivalent to the quadratic equation

$$x^2 + q = px.$$

The original pair was solved by a method that gave the two roots of the quadratic,

$$x, y = \frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q},$$

when both were positive (the Babylonians did not admit negative numbers). The steps in the method were as follows:

- (i) Form $\frac{x+y}{2}$.
- (ii) Form $\left(\frac{x+y}{2}\right)^2$.
- (iii) Form $\left(\frac{x+y}{2}\right)^2 - xy$.
- (iv) Form $\sqrt{\left(\frac{x+y}{2}\right)^2 - xy} = \frac{x-y}{2}$.
- (v) Find x, y by inspection of the values in (i), (iv).

(See Boyer (1968), p. 34, for an actual example.) Of course, these steps were not expressed in symbols but only applied to specific numbers. Nevertheless, a general method is implicit in the many specific cases solved.

An explicit general method, expressed as a formula in words, was given by Brahmagupta (628):

To the absolute number multiplied by four times the [coefficient of the] square, add the square of the [coefficient of the] middle term; the square root of the same, less the [coefficient of the] middle term, being divided by twice the [coefficient of the] square is the value.

Colebrooke (1817), p. 346

This is the solution

$$x = \frac{\sqrt{4ac + b^2} - b}{2a}$$

of the equation

$$ax^2 + bx = c,$$

yet one wonders whether Brahmagupta understood it quite this way when, a few lines later, he gives another rule that is trivially equivalent to the first when expressed in our notation:

$$x = \frac{\sqrt{ac + (b/2)^2} - (b/2)}{a}.$$

The methods of the Babylonians and Brahmagupta clearly give correct solutions, but their basis is not clear. The meaning of square roots, for example, was not questioned as it was by Greeks. A rigorous basis for the solution of quadratic equations can be found in Euclid's *Elements*, Book VI. His Proposition 28 can be viewed as a solution of the general quadratic equation in the case where there is a positive root, as Heath (1925), Vol. 2, p. 263 explains. However, the algebraic interpretation is far from obvious even when one specializes the proposition, which is about parallelograms, to one about rectangles. It seems unlikely that Euclid was aware of the algebra, or he would have expressed it by much simpler geometry.

The transition from geometry to algebra can be seen in al-Khwārizmī's solution of a quadratic equation (Figure 5.1). The solution is still expressed in geometric language, but now the geometry is a direct embodiment of the algebra. It is really the standard algebraic solution, but with “squares” and “products” understood literally as geometric squares and rectangles. To solve $x^2 + 10x = 39$, represent x^2 by a square of side x , and $10x$ by two $5 \times x$ rectangles as in Figure 5.1. The extra square of area 25 “completes the square” of side $x + 5$ to one of area $25 + 39$, since 39 is the given value of $x^2 + 10x$. Thus the big square has area 64, hence its side $x + 5$ equals 8. This gives the solution $x = 3$.

Euclid and al-Khwārizmī did not admit negative lengths, so the solution $x = -13$ to $x^2 + 10x = 39$ does not appear. This is quite natural, since geometry admits only one square with area 64. Avoiding negative coefficients, however, causes algebraic complications. There is not one general quadratic equation, but three, corresponding to the different ways of distributing positive terms between the two sides: $x^2 + ax = b$, $x^2 = ax + b$, $x^2 + b = ax$.

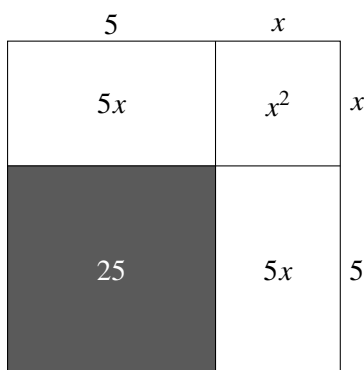


Figure 5.1: Solving a quadratic equation

EXERCISES

Quadratic equations arise frequently in geometry because distance is governed by a quadratic equation (ultimately, by the Pythagorean theorem). In fact, the points created from rational points by any ruler and compass construction can be found by solving a series of linear or quadratic equations, which is why they can be expressed by rational operations and square roots. This result, which was claimed in Section 2.3, can be proved as follows.

5.3.1 Show that the line through two rational points has an equation with rational coefficients.

5.3.2 Show that a circle whose center is a rational point and whose radius is rational has an equation with rational coefficients.

Your proof should show, more generally, that a line or circle constructed from *any* points has an equation with coefficients obtainable from the coordinates of the given points by rational operations. It then suffices to show that intersections of lines and circles can be obtained from the coefficients of their equations by rational operations and square roots.

5.3.3 Show that the intersection of two lines can be computed by rational operations.

5.3.4 Show that the intersection of a line and a circle can be computed by rational operations and a square root (because it depends on solving a quadratic equation).

The last, and hardest, case is finding the intersection of two circles. Fortunately, it is easy to reduce these two quadratic equations to the case just handled in Exercise 5.3.4.

5.3.5 The equations of any two circles can be written in the form

$$(x - a)^2 + (y - b)^2 = r^2,$$

$$(x - c)^2 + (y - d)^2 = s^2.$$

Explain why. Now subtract one of these equations from the other, and hence show that their common solutions can be found by rational operations and square roots.

When a sequence of quadratic equations is solved, the solution may involve *nested* square roots, such as $\sqrt{(5 + \sqrt{5})/2}$. This very number, in fact, occurs in the icosahedron, as one sees from Pacioli's construction in Section 2.2.

5.3.6 Show that the diagonal of a golden rectangle (which is also the diameter of an icosahedron of edge length 1) is $\sqrt{(5 + \sqrt{5})/2}$.

5.4 Quadratic Irrationals

The roots of quadratic equations with rational coefficients are numbers of the form $a + \sqrt{b}$, where a, b are rational. Euclid took the theory of irrationals further in Book X of the *Elements* with a very detailed study of numbers of the form $\sqrt{a \pm \sqrt{b}}$, where a, b are rational. Book X is the longest book in the *Elements* and it is not clear why Euclid devoted so much space to this topic: perhaps because some of it is needed for the study of regular polyhedra in Book XIII (see Section 2.2 and Exercise 5.3.6), perhaps simply because it was Euclid's favorite topic, or perhaps it was one in which he had some original contributions to show off. It is said that Apollonius took the theory of irrationals further, but unfortunately his work on the subject is lost.

After this, there seems to have been no progress in the theory of irrationals until the Renaissance, except for a remarkable isolated result by Fibonacci (1225). Fibonacci showed that the roots of $x^3 + 2x^2 + 10x = 20$ are not any of Euclid's irrationals. This is *not* a proof, as some historians have thought, that the roots cannot be constructed by ruler and compass. Fibonacci did not rule out *all* expressions built from rationals and square roots; nevertheless, it was the first step into the world of irrationals beyond Euclid.

At this point it is worth asking how difficult it is to show that a specific number, say, $\sqrt[3]{2}$, cannot be constructed from rational numbers by

square roots. The answer will depend on how well the reader manages the following exercises. The manipulation required would certainly not have been beyond the 16th-century algebraists. The subtle part is finding a suitable classification of expressions according to complexity—extending Euclid’s classification to expressions in which radical signs are nested to arbitrary depth—and using induction on the level of complexity. This type of thinking did not emerge until the 1820s, hence the relatively late proof that $\sqrt[3]{2}$ is not constructible by ruler and compass, by Wantzel (1837). A few decades later, the proof became a routine part of the theory of fields and vector spaces, as we will see in Chapter 16.

EXERCISES

An elementary proof that $\sqrt[3]{2}$ is not constructible was found by the number theorist Edmund Landau (1877–1938) when he was still a student. It is broken down to easy steps below. But first we should check that $\sqrt[3]{2}$ is actually irrational.

5.4.1 Show that the assumption $\sqrt[3]{2} = m/n$, where m and n are integers, leads to a contradiction.

Landau’s proof now organizes all numbers involved in a construction into sets F_0, F_1, F_2, \dots , according to the depth of nesting of square roots.

5.4.2 Let

$$F_0 = \{\text{rationals}\}, \quad F_{k+1} = \{a + b\sqrt{c_k} : a, b, c_k \in F_k\} \quad \text{for some } c_k \in F_k.$$

Show that each F_k is a *field*, that is, if x, y are in F_k , then so are $x + y$, $x - y$, xy , and x/y (for $y \neq 0$).

We know from Exercise 5.4.1 that $\sqrt[3]{2}$ is not in F_0 , but if it is constructible it will occur in some F_{k+1} . A contradiction now ensues by considering (hypothetically) the first such F_{k+1} .

5.4.3 Show that if $a, b, c \in F_k$ but $\sqrt{c} \notin F_k$, then $a + b\sqrt{c} = 0 \Leftrightarrow a = b = 0$. (For $k = 0$ this is in the *Elements*, Book X, Prop. 79.)

5.4.4 Suppose $\sqrt[3]{2} = a + b\sqrt{c}$, where $a, b, c \in F_k$, but that $\sqrt[3]{2} \notin F_k$. (We know that $\sqrt[3]{2} \notin F_0$ from Exercise 5.4.1.) Cube both sides and deduce from Exercise 5.4.3 that

$$2 = a^3 + 3ab^2c \quad \text{and} \quad 0 = 3a^2b + b^3c.$$

5.4.5 Deduce from Exercise 5.4.4 that $\sqrt[3]{2} = a - b\sqrt{c}$ also, and explain why this is a contradiction.

5.5 The Solution of the Cubic

In our own days Scipione del Ferro of Bologna has solved the case of the cube and first power equal to a constant, a very elegant and admirable accomplishment. Since this art surpasses all human subtlety and the perspicuity of mortal talent and is a truly celestial gift and a very clear test of the capacity of men's minds, whoever applies himself to it will believe that there is nothing that he cannot understand. In emulation of him, my friend Niccolò Tartaglia of Brescia, wanting not to be outdone, solved the same case when he got into a contest with his [Scipione's] pupil, Antonio Maria Fior, and, moved by my many entreaties, gave it to me ... having received Tartaglia's solution and seeking a proof of it, I came to understand that there were a great many other things that could also be had. Pursuing this thought and with increased confidence, I discovered these others, partly by myself and partly through Lodovico Ferrari, formerly my pupil.

Cardano (1545), p. 8

The solution of cubic equations in the early 16th century was the first clear advance in mathematics since the time of the Greeks. It revealed the power of algebra that the Greeks had not been able to harness, power that was soon to clear a new path to geometry, which was virtually a royal road (algebraic geometry and calculus). Cardano's elation at the discovery was well-founded. Even in the 20th century, personally discovering the solution of the cubic equation has been the inspiration for at least one distinguished mathematical career—see Kac (1984).

As for the history of the original discovery, we know little more than Cardano tells us. Scipione del Ferro died in 1526, so the first solution was known before then. Tartaglia discovered his solution on February 12, 1535, probably independently, because he solved all problems in the contest with del Ferro's pupil Fior, while Fior did not. Cardano has been accused by almost everyone, from Tartaglia on, of stealing Tartaglia's solution, but his own account seems to distribute credit quite fairly. For more background, see the introduction and preface to Cardano (1545) and Crossley (1987).

Cardano presents algebra in the geometric style of al-Khwārizmī (whom he describes as the originator of algebra at the beginning of the book), with

the case distinctions caused by avoiding negative coefficients. Ignoring these complications, his solution can be described as follows. The cubic equation $x^3 + ax^2 + bx + c = 0$ is first transformed into one with no quadratic term by a linear change of variable, $x = y - a/3$. One then has, say,

$$y^3 = py + q.$$

By setting $y = u + v$, the left-hand side becomes

$$(u^3 + v^3) + 3uv(u + v) = 3uvy + (u^3 + v^3),$$

which equals the previous right-hand side if

$$\begin{aligned} 3uv &= p, \\ u^3 + v^3 &= q. \end{aligned}$$

Eliminating v gives a quadratic in u^3 ,

$$u^3 + \left(\frac{p}{3u}\right)^3 = q,$$

with roots

$$\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}.$$

By symmetry, we obtain the same values for v^3 . And since $u^3 + v^3 = q$, if one of the roots is taken to be u^3 , the other is v^3 . Without loss of generality we can take

$$\begin{aligned} u^3 &= \frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}, \\ v^3 &= \frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}, \end{aligned}$$

and hence

$$y = u + v = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}} + \sqrt[3]{\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}}.$$

EXERCISES

The two equations $3uv = p$, $u^3 + v^3 = q$ provide another instance of the phenomenon noted in Exercise 5.2.2: when a variable is eliminated between two equations, the degrees of the equations are multiplied.

5.5.1 The equation $3uv = p$ is of degree 2 in u and v , and $u^3 + v^3 = q$ is of degree 3. What about the equation obtained by eliminating v ?

The Cardano formula produces some surprising results, which we look at again in Section 11.2. But first let us test it on a really simple cubic equation.

5.5.2 Use Cardano's formula to solve $y^3 = 2$. Do you get the obvious solution?

Now try one where the solution is less obvious.

5.5.3 Use Cardano's formula to solve $y^3 = 6y + 6$, and check your answer by substitution.

5.6 Angle Division

Another important contributor to algebra in the 16th century was Viète (1540–1603). He helped emancipate algebra from the geometric style of proof by introducing letters for unknowns and using plus and minus signs to facilitate manipulation. Yet at the same time he strengthened its ties with geometry at a higher level by relating algebra to trigonometry. A case in point is his solution of the cubic by circular functions (Viète (1591), Ch. VI, Theorem 3), which shows that solving the cubic is equivalent to trisecting an arbitrary angle.

Namely, if we take the cubic in the form

$$x^3 + ax + b = 0,$$

we can reduce it to an equation

$$4y^3 - 3y = c$$

with just one parameter, by setting $x = ky$ and choosing k so that

$$\frac{k^3}{ak} = \frac{-4}{3}, \quad \text{or} \quad k = \sqrt{\frac{-4a}{3}}.$$

The point of the expression $4y^3 - 3y$ is that

$$4\cos^3\theta - 3\cos\theta = \cos 3\theta;$$

so by setting $y = \cos\theta$ we obtain

$$\cos 3\theta = c.$$

If we are given c , then we can construct a triangle with angle $\cos^{-1} c = 3\theta$. Trisection of this angle gives us the solution $y = \cos \theta$ of the equation. Conversely, the problem of trisecting an angle with cosine c is equivalent to solving the cubic equation $4y^3 - 3y = c$.

Of course, there is a problem with trigonometric interpretation when $|c| > 1$, which requires complex numbers for its resolution. Complex numbers are also involved in Cardano's formula, since the expression under the square root sign, $(q/2)^2 - (p/3)^3$, can be negative. In fact, Viète's method requires complex numbers only when Cardano's does not, so between the two of them, complex numbers are avoided. Nevertheless, cubic equations are the birthplace of complex numbers, as we will see in Chapter 11.

Astonishingly, the problem of dividing an angle into any odd number of equal parts has an algebraic solution analogous to the algebraic solution of the cubic. Viète (1579) himself took the problem as far as finding expressions for $\cos n\theta$ and $\sin n\theta$ as polynomials in $\cos \theta$ and $\sin \theta$, at least for certain values of n . Newton read Viète in 1663–4 and found the equation

$$y = nx - \frac{n(n^2 - 1)}{3!}x^3 + \frac{n(n^2 - 1)(n^2 - 3^2)}{5!}x^5 + \dots$$

relating $y = \sin n\theta$ and $x = \sin \theta$ (see Newton (1676a) in Turnbull (1960)). He asserted this result for arbitrary n , but we are interested in the case of odd integral n , when it reduces to a polynomial equation of degree n . The surprise is that Newton's equation then has a solution by n th roots analogous to the Cardano formula for cubics,

$$x = \frac{1}{2} \sqrt[n]{y + \sqrt{y^2 - 1}} + \frac{1}{2} \sqrt[n]{y - \sqrt{y^2 - 1}}, \quad (1)$$

although only for n of the form $4m + 1$. This formula appears out of the blue in de Moivre (1707).¹ He does not explain how he found it, but it is comprehensible to us as

$$\sin \theta = \frac{1}{2} \sqrt[n]{\sin n\theta + i \cos n\theta} + \frac{1}{2} \sqrt[n]{\sin n\theta - i \cos n\theta}, \quad (2)$$

a consequence of *our* version of de Moivre's formula

$$(\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta \quad (3)$$

¹It also appears in the unpublished Leibniz (1675), though without the restriction on n . See Schneider (1968), pp. 224–228.

when $n = 4m + 1$. (See Exercises 5.6.2 and 5.6.3.)

Viète himself came remarkably close to (3) in a posthumously published work, Viète (1615). He observed that the products of $\sin \theta$, $\cos \theta$ that occur in $\cos n\theta$, $\sin n\theta$ are the alternate terms in the expansion of $(\cos \theta + \sin \theta)^n$, except for certain minus signs. He failed only to notice that the signs could be explained by giving $\sin \theta$ the coefficient i . In any case, such an explanation would not have seemed natural to his contemporaries, who were far more comfortable with Cardano's formula than they were with i . In Section 12.1 we will see how de Moivre's formula evolved with the development of complex numbers.

EXERCISES

A good use of de Moivre's formula is to prove the formula for $\cos 3\theta$ involved in Viète's solution of the cubic.

5.6.1 Use $(\cos \theta + i \sin \theta)^3 = \cos 3\theta + i \sin 3\theta$ to find a formula for $\cos 3\theta$.

The reasons why (1) and (2) hold only for certain integer values, while (3) holds for all, can be understood by actually working out $(\sin \theta + i \cos \theta)^n$.

5.6.2 Use (3) and $\sin \alpha = \cos(\pi/2 - \alpha)$, $\cos \alpha = \sin(\pi/2 - \alpha)$ to show that

$$(\sin \theta + i \cos \theta)^n = \begin{cases} \sin n\theta + i \cos n\theta & \text{when } n = 4m + 1 \\ -\sin n\theta - i \cos n\theta & \text{when } n = 4m + 3. \end{cases}$$

5.6.3 Deduce from Exercise 5.6.2 that (2) is correct for $n = 4m + 1$ and false for $n = 4m + 3$, and hence that (1) is a correct relation between $y = \sin n\theta$ and $x = \sin \theta$ only when $n = 4m + 1$.

5.6.4 Show that (1) is a correct relation between $y = \cos n\theta$ and $x = \cos \theta$ for all n (de Moivre (1730)).

5.7 Higher-Degree Equations

The general fourth-degree, or *quartic*, equation

$$x^4 + ax^3 + bx^2 + cx + d = 0$$

was solved by Cardano's student Ferrari, and the solution was published in Cardano (1545), p. 237. A linear transformation reduces the equation to the form

$$x^4 + px^2 + qx + r = 0,$$

or

$$(x^2 + p)^2 = px^2 - qx + p^2 - r.$$

Then for any y ,

$$\begin{aligned}(x^2 + p + y)^2 &= (px^2 - qx + p^2 - r) + 2y(x^2 + p) + y^2 \\ &= (p + 2y)x^2 - qx + (p^2 - r + 2py + y^2).\end{aligned}$$

The quadratic $Ax^2 + Bx + C$ on the right-hand side will be a square if $B^2 - 4AC = 0$, which is a cubic equation for y . We can therefore solve for y and take the square root of both sides of the equation for x , which then becomes quadratic and hence also solvable. The final result is a formula for x using just square and cube roots of rational functions of the coefficients.

This impressive bonus to the solution of cubic equations raised hopes that higher-degree equations could also be solved by formulas built from the coefficients by rational operations and roots, and *solution by radicals*, as it was called, became a major goal of algebra for the next 250 years. However, all such efforts to solve the general equation of fifth degree (quintic) failed. The most that could be done was to reduce it to the form

$$x^5 - x - A = 0$$

with only one parameter. This was done by Bring (1786), and a sketch of his method may be seen in Pierpont (1895). Bring's result appeared in a very obscure publication and went unnoticed for 50 years, or it might have rekindled hopes for the solution of the quintic by radicals. As it happened, Ruffini (1799) offered the first proof that this is impossible. Ruffini's proof was not completely convincing, but he was vindicated when a satisfactory proof was given by Abel (1826), and again with the beautiful general theory of equations of Galois (1831b).

A positive outcome of Bring's result was the analytic solution of the quintic by Hermite (1858). Reduction to an equation with one parameter opened the way to a solution by transcendental functions, like Viète's solution of the cubic by circular functions. Suitable functions, the elliptic modular functions, had been discovered by Gauss, Abel, and Jacobi, and Galois (1831a) had hinted at their relation to quintic equations. This extraordinary confluence of ideas was the subject of Klein (1884).

In view of the difficulties with the quintic, there was naturally very little progress with the general equation of degree n . However, two simple but important contributions were made by Descartes (1637). The first was

the superscript notation for powers we now use: x^3 , x^4 , x^5 , and so on. (Though not x^2 , oddly enough. The square of x continued to be written xx until well into the next century.) The second was the theorem of Descartes (1637), p. 159, that a polynomial $p(x)$ with value 0 when $x = a$ has a factor $(x - a)$. Since division of a polynomial $p(x)$ of degree n by $(x - a)$ leaves a polynomial of degree $n - 1$, Descartes's theorem raised the hope of factorizing each n th-degree polynomial into n linear factors. As Chapter 11 shows, this hope was fulfilled with the development of complex numbers.

EXERCISES

The main steps in the proof of Descartes's theorem go as follows. If the first step does not seem sufficiently easy, begin with $a = 1$.

5.7.1 Show that $x^n - a^n$ has a factor $x - a$. What is the quotient $(x^n - a^n)/(x - a)$? (And what does this have to do with geometric series?)

5.7.2 If $p(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0$, use Exercise 5.7.1 to show that $p(x) - p(a)$ has a factor $x - a$.

5.7.3 Deduce Descartes's theorem from Exercise 5.7.2.

5.8 The Binomial Theorem

Some important results in algebra/number theory were discovered in the Middle Ages, though they failed to take root until they were rediscovered in the 17th century or later. Among these were the discovery of “Pascal's triangle” by Chinese mathematicians, and formulas for permutations and combinations by Levi ben Gershon (1321). Pascal's triangle began to flourish in the 17th century after a long dormancy, so it is of interest to see what was known of it in medieval times and what Pascal did to revive it.

The Chinese used Pascal's triangle to generate and tabulate the binomial coefficients, that is, the coefficients in the formulas

$$\begin{aligned}
 (a + b)^1 &= a + b \\
 (a + b)^2 &= a^2 + 2ab + b^2 \\
 (a + b)^3 &= a^3 + 3a^2b + 3ab^2 + b^3 \\
 (a + b)^4 &= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4 \\
 (a + b)^5 &= a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5 \\
 (a + b)^6 &= a^6 + 6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 + b^6 \\
 (a + b)^7 &= a^7 + 7a^6b + 21a^5b^2 + 35a^4b^3 + 35a^3b^4 + 21a^2b^5 + 7ab^6 + b^7
 \end{aligned}$$

and so on. When the binomial coefficients are tabulated as follows (with a trivial row 1 added at the top, corresponding to the power 0 of $a + b$),

$$\begin{array}{ccccccc}
 & & & & 1 & & \\
 & & & 1 & & 1 & \\
 & & 1 & & 2 & & 1 \\
 & 1 & & 3 & & 3 & & 1 \\
 & & 1 & & 4 & & 6 & & 4 & & 1 \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
 & 1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1
 \end{array}$$

and so on, the k th element $\binom{n}{k}$ of the n th row is the sum $\binom{n-1}{k-1} + \binom{n-1}{k}$ of the two elements above it in the $(n-1)$ th row, as follows from the formula (Exercise 5.8.1)

$$(a+b)^n = (a+b)^{n-1}a + (a+b)^{n-1}b.$$

The triangle appears to a depth of six in Yáng Huí (1261) and to a depth of eight in Zhū Shijié (1303) (Figure 5.2). Yáng Huí attributes the triangle to Jia Xiàn, who lived in the 11th century.

The number $\binom{n}{k}$ appears in medieval Hebrew writings as the number of combinations of n things taken k at a time. Levi ben Gershon (1321) gives the formula

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

together with the fact that there are $n!$ permutations of n elements.

In view of these excellent results, why do we call the table of binomial coefficients Pascal's triangle? It is of course not the only instance of a mathematical concept being named after a rediscoverer rather than a discoverer, but in any case Pascal deserves credit for more than just rediscovery. In his *Traité du triangle arithmétique*, Pascal (1654) united the algebraic and combinatorial theories by showing that the elements of the arithmetic triangle could be interpreted in two ways: as the coefficients of $a^{n-k}b^k$ in $(a+b)^n$ and as the number of combinations of n things taken k at a time. As an application, he founded the mathematical theory of probability by solving the problem of division of stakes (Exercise 5.8.2), and as a method of proof he consciously used mathematical induction (in

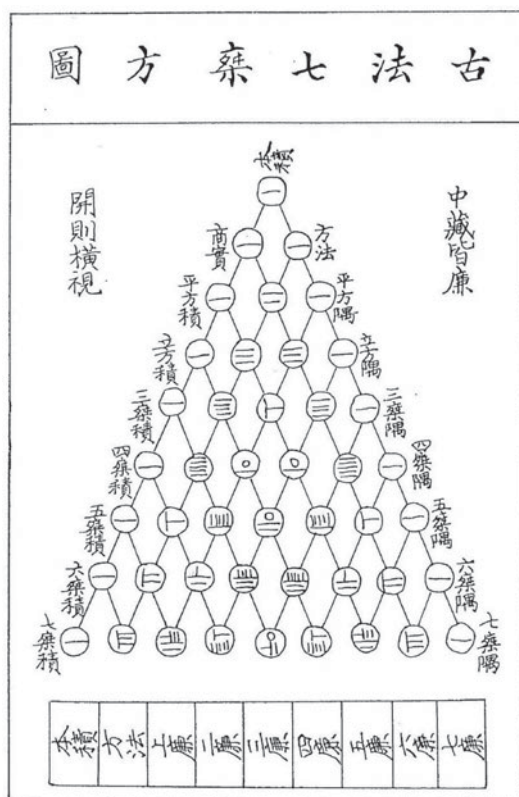


Figure 5.2: Chinese Pascal's triangle

the “base step, induction step” format) for the first time. Altogether, quite some progress!

EXERCISES

The basic properties of the binomial coefficients, for example the fact that each is the sum of the two above it in Pascal's triangle, follow easily from their interpretation as the coefficients in the expansion of $(a + b)^n$.

5.8.1 Use the identity

$$(a+b)^n = (a+b)^{n-1}a + (a+b)^{n-1}b$$

to prove the sum property of binomial coefficients:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

This property gives an easy way to calculate Pascal's triangle to any depth, and hence compute a fair division of stakes in a game that has to be called off with n plays remaining. We suppose that players I and II have an equal chance of winning each play, and that I needs to win k of the remaining n plays to carry off the stakes.

5.8.2 Show that the ratio of I's winning the stakes to that of II's winning is

$$\binom{n}{n} + \binom{n}{n-1} + \cdots + \binom{n}{k} : \binom{n}{k-1} + \binom{n}{k-2} + \cdots + \binom{n}{0}.$$

The sum property of the binomial coefficients also explains the presence of some interesting numbers in Pascal's triangle.

5.8.3 Explain why the third diagonal from the left in the triangle, namely 1, 3, 6, 10, 15, 21, ..., consists of the triangular numbers.

5.8.4 The numbers on the next diagonal, namely 1, 4, 10, 20, 35, ..., can be called *tetrahedral numbers*. Why is this an apt description?

5.9 Fermat's Little Theorem

The algebra of binomial coefficients also led to a famous theorem of number theory due to Fermat (1640). It is known as his "little" or "lesser" theorem to distinguish it from his "last" or "great" theorem (Section 10.1). Fermat's little theorem is the following.

If p is prime and $\gcd(n, p) = 1$, then $n^{p-1} - 1$ is divisible by p or, equivalently, $n^p - n$ is divisible by p .

The equivalence holds because $n^p - n = n(n^{p-1} - 1)$ is divisible by p if and only if $n^{p-1} - 1$ is, since p is prime and does not divide n .

Fermat's little theorem has recently become indispensable in areas of applied mathematics, such as cryptography, so it is thought-provoking to learn that it originated in one of the least applied problems in mathematics, the construction of perfect numbers. As we saw in Section 3.2, this depends on the construction of prime numbers of the form $2^m - 1$, and it was initially for this reason that Fermat became interested in conditions for $2^m - 1$ to have divisors. At the same time (mid-1630s) he was investigating the binomial coefficients, and the combination of these two interests very likely led to the discovery of his little theorem, for $n = 2$.

His actual proof is unknown, but various authors (for example, Weil (1984), p. 56) have pointed out that the theorem follows immediately from

the fact that $\binom{p}{1}, \binom{p}{2}, \dots, \binom{p}{p-1}$, for p prime, are divisible by p :

$$2^p = (1 + 1)^p = 1 + \binom{p}{1} + \binom{p}{2} + \dots + \binom{p}{p-1} + 1,$$

hence

$$2^p - 2 = \binom{p}{1} + \binom{p}{2} + \dots + \binom{p}{p-1}$$

is divisible by p , and therefore so is $2^{p-1} - 1$.

But how does one prove that $\binom{p}{1}, \binom{p}{2}, \dots, \binom{p}{p-1}$ are divisible by p ? This follows easily from the Levi ben Gershon formula

$$\binom{p}{k} = \frac{p!}{(p-k)!k!},$$

which shows that the prime p is a factor of the numerator but not of the denominator. The denominator nevertheless divides the numerator, since $\binom{p}{k}$ is an integer, so (by unique prime factorization) the factor p must remain after the division has taken place. Fermat may not have had precisely this result, since he did not yet have Pascal's combinatorial interpretation of the binomial coefficients, but he did have the formula

$$n \binom{n+m-1}{m-1} = m \binom{n+m-1}{m},$$

which implies it and from which the divisibility property may be extracted (see Weil (1984), p. 47).

Thus far we have a proof of Fermat's little theorem for $n = 2$. Weil (1984) suggests two possible routes to the general theorem from this point. One is by iteration of the binomial theorem, a method that was used in the first published proof of Fermat's theorem by Euler (1736). The other is by direct application of the *multinomial theorem*, the method of the earliest known proof, which is in an unpublished paper of Leibniz from the late 1670s (see Weil (1984), p. 56).

Just as

$$\text{coefficient of } a^{p-k}b^k \text{ in } (a+b)^p = p!/(p-k)!k!,$$

$$\text{coefficient of } a_1^{q_1}a_2^{q_2}\cdots a_n^{q_n} \text{ in } (a_1+a_2+\cdots+a_n)^p = p!/q_1!q_2!\cdots q_n!,$$

where $q_1 + q_2 + \cdots + q_n = p$ (Exercise 5.9.4). This *multinomial coefficient* is divisible by p , by the same argument as before, provided no $q_i = p$. Thus the coefficients of all but $a_1^p, a_2^p, \dots, a_n^p$ in $(a_1 + a_2 + \cdots + a_n)^p$ are divisible by the prime p . It follows, by replacing each of the n terms a_1, a_2, \dots, a_n by 1, that

$$(1 + 1 + \cdots + 1)^p = 1^p + 1^p + \cdots + 1^p + \text{terms divisible by } p,$$

that is, $n^p - n$ is divisible by p . Then if n itself is relatively prime to p (hence not divisible by p), we have $n^{p-1} - 1$ divisible by p , or the general Fermat little theorem.

EXERCISES

The binomial theorem may be iterated to show that p divides $n^p - n$ as follows.

5.9.1 Use the result $2^p = (1 + 1)^p = 2 + \text{terms divisible by } p$, and its method of proof, to show that

$$3^p = (2 + 1)^p = 3 + \text{terms divisible by } p.$$

5.9.2 Build on the idea of Exercise 5.9.1 to show that $n^p - n$ is divisible by p for any positive integer n .

5.9.3 Observe the terms divisible by p in the first few rows of Pascal's triangle, computed in the previous section.

Like the binomial theorem, the multinomial theorem can be proved combinatorially by considering the number of ways a term $a_1^{q_1} a_2^{q_2} \cdots a_n^{q_n}$ can arise from the factors of $(a_1 + a_2 + \cdots + a_n)^p$.

5.9.4 Prove the formula for the multinomial coefficient given above by observing that the coefficient equals the number of ways of partitioning p things into disjoint subsets of sizes q_1, q_2, \dots, q_n .



6

Algebraic Geometry

PREVIEW

The first field of mathematics to benefit from the new language of equations was geometry. Around 1630, both Fermat and Descartes realized that geometric problems could be translated into algebra by means of *coordinates*, and that many problems could then be routinely solved by algebraic manipulation.

The language of equations also provides a simple but natural classification of curves by *degree*. The curves of degree 1 are the straight lines; the curves of degree 2 are the conic sections; so the first “new” curves are those of degree 3, the *cubic curves*.

Cubic curves exhibit new geometric features—cusps, inflections, and self-intersections—so they are considerably more complicated than the conic sections. Nevertheless, Newton attempted to classify them, and in doing so he discovered that cubic curves, when properly viewed, are not as complicated as they seem.

We will find our way to the “right” viewpoint in Chapters 7 and 11. In the meantime we discuss another theorem that depends on the “right” viewpoint: *Bézout’s theorem*, according to which a curve of degree m always meets a curve of degree n in mn points.

6.1 Steps Toward Algebraic Geometry

The basic idea of algebraic geometry is the representation of curves by equations, but this is not the whole idea. If it were, then the Greeks would be considered the first algebraic geometers. Menaechmus was perhaps the first to discover (what we would call) equations of curves, along with his discovery of the conic sections. We have seen how equations explain how he obtained $\sqrt[3]{2}$ as the intersection of a parabola and a hyperbola (Section 2.4). Apollonius' study of conics involved equations, but they were arrived at by geometric arguments.

What was lacking in Greek mathematics was both the inclination and the technique to manipulate equations to obtain information about curves. The Greeks used curves to study algebra rather than the other way around. Menaechmus's construction of $\sqrt[3]{2}$ is a fine example of this: extraction of roots was not a given algebraic operation but one achieved by geometric construction. Similarly, an equation was not an entity in its own right but a property of a curve that could be discovered after the curve had been constructed geometrically. This was natural as long as equations were written in words. When, as in Apollonius, an equation takes half a page to write out, it is difficult to form a general concept of equation, function, or curve. Hence the lack of a general concept of curve in Greek mathematics—it was just too complicated to handle in their language.

Also lacking was an appreciation of *coordinates* in geometry. Coordinates had been used in astronomy and geography since Hipparchus (around 150 BCE); but they were not used to describe functions or curves until the Middle Ages, in the work of Oresme (around 1323–1382). Oresme still called the coordinates “longitude” and “latitude,” but he used them to represent functions such as velocity as a function of time. Setting up the coordinate system *before* determining the curve was Oresme's step beyond the Greeks, but he too lacked the algebra to go further.

The step that finally made algebraic geometry feasible was the solution of equations and the improvement of notation in the 16th century, which we discussed in the previous chapter. This step made it possible to consider equations, and hence curves, in some generality and to manipulate them fluently. As we will see in the next section, the two founders of algebraic geometry, Fermat and Descartes, both exploited these developments.

For more on the early history of algebraic geometry, see the book Boyer (1956) and the first chapter of Brieskorn and Knörrer (1981).

It may be worth mentioning, at this point, that this kind of geometry has traditionally been called “analytic” rather than “algebraic.” We are calling the geometry “algebraic” to emphasize that its *objects* are algebraically defined (by polynomial equations) and that they are investigated by *methods* of algebra. This is also in line with modern use of the term “algebraic geometry.” The methods of analysis come into play only later, particularly for curves defined by nonalgebraic means, which Descartes called “mechanical.” The term “analytic geometry” is better employed for the latter, more general, kind of geometry.

EXERCISE

6.1.1 Generalize the idea of Menaechmus to show that any cubic equation

$$ax^3 + bx^2 + cx + d = 0 \quad \text{with} \quad d \neq 0$$

may be solved by intersecting the hyperbola $xy = 1$ with a parabola.

6.2 Fermat and Descartes

There have been several occasions in the history of mathematics when an important discovery was made independently and almost simultaneously by two individuals: non-Euclidean geometry by Bolyai and Lobachevsky, elliptic functions by Abel and Jacobi, the calculus by Newton and Leibniz, for example. To the extent that we can rationally explain these remarkable events, it is on the basis of ideas already “in the air,” and conditions becoming favorable for their precipitation. As I tried to show in the previous section, conditions were favorable for algebraic geometry at the beginning of the 17th century. So it is not completely surprising that the subject was independently discovered by Fermat (1629) and Descartes (1637). (Descartes’s work *La Géométrie* may in fact have been started in the 1620s. In any case it is independent of Fermat, whose work was not published until 1679.)

It is surprising, however, that both Fermat and Descartes began with an algebraic solution of the same classical geometric problem, the so-called “four-line problem” of Apollonius, and that the main discovery of each was that second-degree equations correspond to conic sections. Up to this stage Fermat was more systematic than Descartes, but that was as far as he went. He was content to leave his work in a “simple and crude” state, confident that it would grow in stature when nourished by new inventions.

Descartes, on the other hand, treated many higher-degree curves and clearly understood the power of algebraic methods in geometry. He wanted to withhold this power from his contemporaries, however, particularly the rival mathematician Roberval, as he admitted in a letter to Mersenne (see Boyer (1956), p. 104). *La Géométrie* was written to boast about his discoveries, not to explain them. There is little systematic development, and proofs are frequently omitted with a sarcastic remark such as, “I shall not stop to explain this in more detail, because I should deprive you of the pleasure of mastering it yourself” (p. 10). Descartes’s conceit is so great that it is a pleasure to see him come a cropper occasionally, as on p. 91: “The ratios between straight and curved lines are not known, and I believe cannot be discovered by human minds.” He was referring to the then-unsolved problem of determining the length of curves, but he spoke too soon, for in 1657 Neil and van Heuraet found the length of an arc of the semicubical parabola $y^2 = x^3$, and the calculus soon made such problems routine. (A full and interesting account of the story of arc length may be found in Hofmann (1974), Ch. 8.)

EXERCISES

As we now know, all conic sections may be given by the following standard form equations (from Section 2.4):

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \text{ (ellipse),} \quad y = ax^2 \text{ (parabola),} \quad \frac{x^2}{a^2} - \frac{y^2}{b^2} = 1 \text{ (hyperbola).}$$

The reduction of an arbitrary quadratic equation in x and y to one of these forms depends on suitable choice of origin and axes, as Fermat and Descartes discovered. The main steps are outlined in the following exercises.

- 6.2.1** Show that a quadratic form $ax^2 + bxy + cy^2$ may be converted to a form $a'x'^2 + b'y'^2$ by suitable choice of θ in the substitution

$$x = x' \cos \theta - y' \sin \theta,$$

$$y = x' \sin \theta + y' \cos \theta,$$

by checking that the coefficient of $x'y'$ is $(c - a) \sin 2\theta + b \cos 2\theta$.

- 6.2.2** Deduce from Exercise 6.2.1 that, by suitable rotation of axes, any quadratic curve may be expressed in the form $a'x'^2 + b'y'^2 + c'x' + d'y' + e' = 0$.
- 6.2.3** If $b' = 0$, but $a' \neq 0$, show that the substitution $x' = x'' + f$ gives either a standard-form parabola, or the “double line” $x''^2 = 0$.
(Why is this called a “double line,” and is it a section of a cone?)
- 6.2.4** If both a' and b' are nonzero, show that a shift of origin gives the standard form for either an ellipse or a hyperbola, or else a pair of lines.

6.3 Algebraic Curves

I could give here several other ways of tracing and conceiving a series of curved lines, each curve more complex than any preceding one, but I think the best way to group together all such curves and then classify them in order is by recognizing the fact that all points of those curves which we may call “geometric,” that is, those which admit of precise and exact measurement, must bear a definite relation to all points of a straight line, and that this relation must be expressed by means of a single equation.

Descartes (1637), p. 48

In this passage Descartes speaks of what we now call *algebraic curves*. The fact that he calls them “geometric” shows his attachment to the Greek idea that curves are the product of geometric constructions. He is using the notation of equations not to define curves directly but to restrict the notion of geometric construction more severely than the Greeks did, thereby restricting the concept of curve. As we saw in Section 2.5, the Greeks considered some constructions, such as rolling one circle on another, that can produce transcendental curves. Descartes called such curves “mechanical” and found a way to exclude them by his restriction to curves “expressed by means of a single equation.” It becomes clear in the lines following the preceding quotation that he means *polynomial* equations, since he gives a classification of equations by degree.

Descartes’s rejection of transcendental curves was short-sighted, since the calculus soon provided techniques to handle them, but nevertheless it was fruitful to concentrate on algebraic curves. The notion of degree, in particular, was a useful measure of complexity. First-degree curves are the simplest possible, namely, straight lines. Those of second degree are the next simplest, conic sections. With third-degree curves one sees the new phenomena of inflections, double points, and cusps. Inflection and cusp are familiar from $y = x^3$ and $y^2 = x^3$, respectively; we also saw a cusp on the cissoid (Section 2.5). A classical example of a cubic with a double point is the *folium* (leaf) of Descartes (1638),

$$x^3 + y^3 = 3axy.$$

The “leaf” is the closed portion in the positive quadrant; Descartes missed the rest of the curve by ignoring negative coordinates. The complete shape

A whole family of “multileaved” curves was studied by Grandi (1723).

6.3.4 The *roses of Grandi* are given by the polar equations

$$r = a \cos n\theta$$

for integer values of n . Figure 6.2 shows some of these curves, as given by Grandi (1723). Show that the roses of Grandi are algebraic.

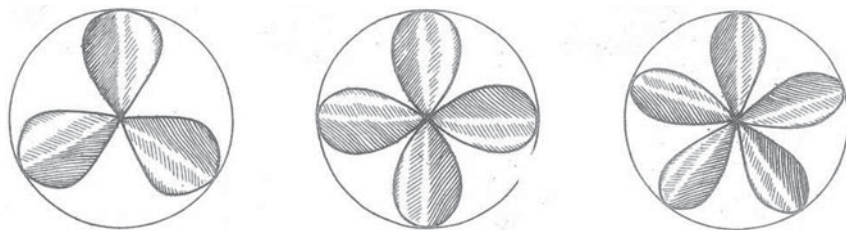


Figure 6.2: Roses of Grandi

6.3.5 Show that the “rose” for $n = 1$ is a circle and that the “rose” for $n = 2$ has cartesian equation

$$(x^2 + y^2)^3 = a^2(x^2 - y^2)^2.$$

6.4 Newton’s Classification of Cubics

Since first- and second-degree curves are straight lines and conics, they were well understood before the advent of algebraic geometry. Up to the end of the 18th century most mathematicians considered them as clear as could be, and hence an unsuitable subject for the new methods. A famous example is the Greek-style treatment of planetary orbits in Newton’s *Principia* (1687). The classical attitude to low-degree curves was summed up by d’Alembert in his article on geometry in the great French *Encyclopédie* (p. 637 of volume 7, 1757):

Algebraic calculation is not to be applied to the propositions of elementary geometry because it is not necessary to use this calculus to facilitate demonstrations, and it appears that there are no demonstrations which can really be facilitated by this calculus except for the solution of problems of second degree by the line and circle.

Thus the first new problem opened up by algebraic geometry, and also the first considered properly to belong to the subject, was the investigation of cubic curves. These curves were classified, more or less completely, by Newton (1695) (see Ball (1890) for a commentary).

Newton (1667) began this work with the general cubic in x and y ,

$$ay^3 + bxy^2 + cx^2y + dx^3 + ey^2 + fxy + gx^2 + hy + kx + l = 0,$$

made a general transformation of axes—which gives an equation with 84 terms (!)—then showed that the equation could be reduced to one of the forms

$$\begin{aligned} Axy^2 + By &= Cx^3 + Dx^2 + Ex + F, \\ xy &= Ax^3 + Bx^2 + Cx + D, \\ y^2 &= Ax^3 + Bx^2 + Cx + D, \\ y &= Ax^3 + Bx^2 + Cx + D. \end{aligned}$$

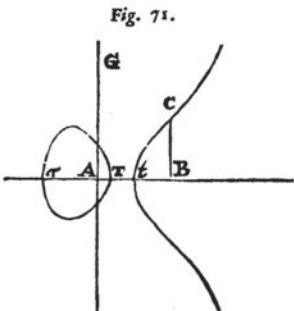
Newton then divided the curves into species according to the roots of the right-hand side, obtaining 72 species (and overlooking 6). His paper lacks detailed proofs; these were supplied by Stirling (1717), along with four of the species Newton missed. Newton's classification was criticized by some later mathematicians, such as Euler, for lacking a general organizing principle. But such a principle was already implicit in one of Newton's passing remarks, Section 29, "On the Genesis of Curves by Shadows." This principle, which will be explained in the next chapter, reduces cubics to the five types seen in Figure 6.3 (taken from an English translation of Newton's paper in Harris (1708); see Whiteside (1964), p. 158).

The reader may wonder where the most familiar cubic, $y = x^3$, appears among these five. The answer is that it is equivalent to the one with a cusp, in Newton's Figure 75. This is explained in the next chapter.

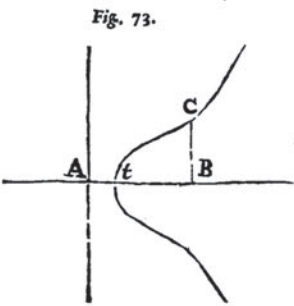
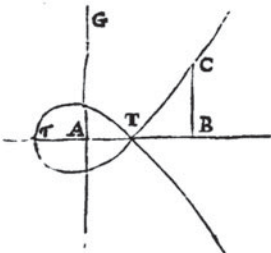
EXERCISES

The cubic curves that Newton called "cuspidate" and "nodated" are algebraically simpler than the others. In particular, they can be parameterized by rational functions.

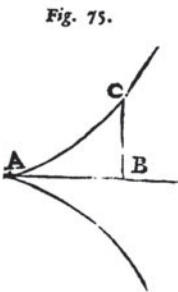
- 6.4.1** Find a parameterization $x = p(t)$, $y = q(t)$ of the semicubical parabola $y^2 = x^3$ by polynomials p and q , (i) by inspection, (ii) by finding the second intersection point of the line $y = tx$ through the cusp $(0, 0)$.
- 6.4.2** Find rational functions $x = r(t)$, $y = s(t)$ that parameterize $y^2 = x^2(x + 1)$, by finding the second intersection of the line $y = tx$ through the double point of the curve.



of the Form of a Bell, with an Oval at its Vertex. And this makes a *Sixty seventh Species*.
If two of the Roots are equal, a Parabola will be formed, either *Nodated* by touching an Oval,

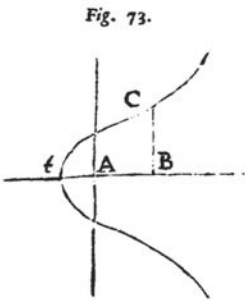


or *Punctate*, by having the Oval infinitely small. Which two *Species* are the *Sixty eighth* and *Sixty ninth*.
If three of the Roots are equal, the Parabola will be *Cuspidate* at the Vertex. And this is the



Neilian Parabola, commonly called Semi-cubical. Which makes the *Seventieth Species*.

If two of the Roots are impossible, there will (See Fig. 73.)



be a *Pure* Parabola of a Bell-like Form. And this makes the *Seventy first Species*.

Figure 6.3: Newton's classification of cubic curves

6.5 Construction of Equations, Bézout's Theorem

In Sections 6.1, 6.2, and 6.3 the development of algebraic geometry is outlined from the first observations of equations as properties of curves to the full realization that equations *define* curves and that the concept of (polynomial) equation is the key to the concept of (algebraic) curve. With hindsight, we can say that Descartes's *La Géométrie* (1637) was a major step in the maturation of the subject, but the book does not conclusively establish what algebraic geometry is. In fact, it is largely devoted to two transitional topics in the development of the subject: the 16th-century theory of equations and the now almost forgotten discipline called “construction of equations.”

The paradigm for construction of an equation was Menaechmus's construction of $\sqrt[3]{2}$ by intersecting a parabola and hyperbola. From a geometric point of view, one is using familiar curves (parabola and hyperbola) to construct a less familiar length ($\sqrt[3]{2}$). This becomes sharper when expressed algebraically: curves of degree 2 are being used to solve an equation of degree 3, $x^3 = 2$. In the 1620s Descartes discovered something more general: a method of solving any third- or fourth-degree equation by intersecting curves of degree 2, a parabola and a circle. His friend Beeckman (1628) reported in a note that “M. Descartes made so much of this invention that he confessed never to have found anything superior himself and even that nobody else had ever found anything better” (translation by Bos (1981), p. 330). Descartes was not as superior as he thought, since Fermat (1629) independently made the same discovery in an unpublished work, strengthening the already extraordinary coincidence between his work and that of Descartes. However, Fermat apparently did not pursue the idea further, and Descartes did.

In *La Géométrie* Descartes found a particular cubic curve, the so-called cartesian parabola, whose intersections with a suitable circle yield the solution of any given fifth- or sixth-degree equation. Descartes concludes the book with this result, blithely telling the reader that

it is only necessary to follow the same method to construct all problems, more and more complex, ad infinitum; for in the case of a mathematical progression, whenever the first two or three terms are given, it is easy to find the rest.

Descartes (1637), p. 240

In reality it was not easy, and efforts to find a satisfactory general construction for n th-degree equations petered out around 1750. The story of the rise and fall of this field of mathematics has been told by Bos (1981, 1984).

In their search for a general construction, mathematicians had casually assumed that a curve of degree m meets a curve of degree n in mn points. The first statement of this principle, which became known as Bézout's theorem, seems to have been made by Newton on May 30, 1665:

For y^e number of points in w^{ch} two lines may intersect can never bee greater y^n y^e rectangle of y^e numbers of their dimensions. And they always intersect in soe many points, excepting those w^{ch} are imaginarie onely.

Newton (1665b), p. 498

Bézout's theorem leads one to hope that solutions of an equation $r(x) = 0$ of degree $k = m \cdot n$ might result from the intersections of a degree m curve with a degree n curve. In algebraic terms, one seeks equations

$$p(x, y) = 0, \quad (1)$$

$$q(x, y) = 0 \quad (2)$$

of degrees m, n respectively, which yield the given equation

$$r(x) = 0 \quad (3)$$

as “resultant” by elimination of y . This is how mathematicians in the West first encountered the problem of elimination, which the Chinese had solved some centuries earlier (Section 5.2).

However, quite apart from the fact that construction of equations was inverse to elimination, and much harder, two more facts about elimination itself were needed: first, that elimination between equations of degrees m and n gave a resultant of degree mn ; second, that an equation of degree mn has mn roots. The second statement, as mentioned in Section 5.7, becomes a fact only when complex numbers are admitted. The first becomes a fact only when “points at infinity” are admitted. If, for example, (1) and (2) are equations of parallel lines, then (3) is of “degree 0” and has *no* solutions. However, one can say that parallel lines meet “at infinity,” and the geometric framework for this idea, projective geometry, developed at about the same time as algebraic geometry. Unfortunately, it was not realized until the 19th century that projective geometry and algebraic geometry needed

each other. Until then, projective geometry developed without coordinates, and all attempts to prove Bézout’s theorem—notably by Maclaurin (1720), Euler (1748b), Cramer (1750), and Bézout (1779)—foundered for want of a proper method for counting points at infinity. As a result, Bézout’s theorem, which turned out to be the main achievement of the theory of construction of equations, was not properly proved until long after the theory itself had been abandoned.

The origins of projective geometry, and the fruits of its merger with algebraic geometry, are discussed in Chapter 7.

EXERCISES

We know from Section 5.7 that an arbitrary quartic equation is equivalent to one of the form

$$x^4 + px^2 + qx + r = 0.$$

6.5.1 Show that any such equation may be solved by finding the intersection of the parabola $y = x^2$ with another quadratic curve (hence with a conic section).

6.5.2 Find two parabolas whose intersections give the solutions of $x^4 = x + 1$, and hence show that this quartic equation has two real roots.

6.6 The Arithmetization of Geometry

We have stressed that early algebraic geometers—Descartes in particular—did not accept that geometry could be *based* on numbers or algebra, even though their work led eventually to this conclusion. Perhaps the first to take the idea of arithmetizing geometry seriously was Wallis (1616–1703). Wallis (1657), Chs. XXIII and XXV, gave the first arithmetic treatment of Euclid’s Books II and V, and Wallis (1655b) had earlier given the first purely algebraic treatment of conic sections. He initially derived equations from the classical definitions by sections of the cone but then proceeded conversely to derive their properties from the equations, “without the embranglings of the cone,” as he put it.

Wallis was ahead of this time. Thomas Hobbes, introduced at the beginning of Chapter 2, described Wallis’s treatise on conics as a “scab of symbols” and denounced “the whole herd of them who apply their algebra of geometry” (Hobbes (1656), p. 316, and Hobbes (1672), p. 447). The example and authority of Newton probably reinforced the opinion that algebra was inappropriate in the geometry of lines or conic sections; we saw in Section 6.4 how this remained the accepted view until at least 1750.

Algebra did not catch on in elementary geometry until it was taken up by Lagrange and supported by influential textbooks of Monge and Lacroix around 1800. But by the time elementary geometry had been brought into the theory of equations, higher geometry had broken out, depending more and more on calculus and the emerging theories of complex functions, abstract algebra, and topology, which bloomed in the 19th century. Higher geometry broke away to form the separate fields of differential geometry and algebraic geometry, leaving the elementary residue we call “analytic geometry” today.

Despite its lowly status, analytic geometry was given an important foundational role by Hilbert (1899). Hilbert took Wallis’s arithmetization to its logical conclusion by assuming only the real numbers and sets as given and constructing *Euclidean geometry* from them.

Thus from the set \mathbb{R} of reals, one constructs the *Euclidean plane* as the set of ordered pairs (x, y) (“points”) where $x, y \in \mathbb{R}$. A *straight line* is a set of points (x, y) in the plane such that $ax + by + c = 0$ for some constants a, b, c . Lines are *parallel* if their x and y coefficients are proportional. The *distance* between points (x_1, y_1) and (x_2, y_2) is defined to be $\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$. This definition is motivated by the Pythagorean theorem, which is the keystone in the bridge from arithmetic to geometry.

With these definitions, all axioms and propositions of Euclid’s geometry become provable propositions about equations. For example, the axiom that nonparallel lines have a point in common corresponds to the theorem that linear equations

$$\begin{aligned}a_1x + b_1y + c_1 &= 0, \\a_2x + b_2y + c_2 &= 0\end{aligned}$$

have a solution when $a_1b_2 - b_1a_2 \neq 0$.

Hilbert did not believe, any more than Newton did, that numbers were the true subject matter of geometry. He supported geometric intuition as a method of discovery, as the book Hilbert and Cohn-Vossen (1932) makes clear. The purpose of arithmetization was to give a secure logical foundation to geometry after the 19th-century developments that discredited geometry and installed arithmetic as the ultimate authority in mathematics. This foundation is no longer quite as secure as it seemed in 1900, as we will see in Chapter 17; nevertheless, it is still the most secure and convenient foundation for the many branches of geometry and analysis.



7

Projective Geometry

PREVIEW

At about the same time as the algebraic revolution in classical geometry, a new kind of geometry also came to light: *projective* geometry. Based on the idea of projecting objects from space to a plane, or from one plane to another, projective geometry was initially the concern of artists. In the 17th century, only a handful of mathematicians were interested in it, and their discoveries were not seen to be important until the 19th century.

The fundamental quantities of classical geometry, such as length and angle, are not preserved by projection, so they have no meaning in projective geometry. Projective geometry can discuss only things that are preserved by projection, such as points and lines.

Surprisingly, there are nontrivial theorems about points and lines. One was discovered by the Greek geometer Pappus around 300 CE, and another by the French mathematician Desargues around 1640.

Even more surprisingly, there is a *numerical* quantity preserved by projection. It is a “ratio of ratios” of lengths called the *cross-ratio*. In projective geometry, the cross-ratio plays a role similar to that played by length in classical geometry.

One of the virtues of projective geometry is that it simplifies the classification of curves. All conic sections, for example, are “projectively the same,” and there are only five types of cubic curve.

The projective viewpoint also removes some apparent exceptions to the theorem of Bézout. For example, a line (curve of degree 1) always meets another line in exactly one point, because in projective geometry even parallel lines meet.

7.1 Perspective

Perspective may be simply described as the realistic representation of spatial scenes on a plane. This of course has been a concern of painters since ancient times, and some Roman artists seem to have achieved correct perspective by the first century BCE; an impressive example is shown in Wright (1983), p. 38. However, the vast majority of ancient paintings show incorrect perspective. If there was ever a classical theory of perspective, it was well and truly lost during the Dark Ages. Medieval artists made some charming attempts at perspective but always got it wrong. See Figure 7.1, for example, which is in *The Lives of Sts. Edmund and Fremund* by John Lydgate, from around 1434, now in the British Library.



Figure 7.1: Errors in perspective

The first correct perspective method is usually attributed to the Florentine painter–architect Brunelleschi (1377–1446), around 1420. The first published method appears in the treatise *On Painting* by Alberti (1436). The latter method, which became known as *Alberti's veil*, used a piece of transparent cloth fixed in front of the scene to be painted. Then, viewing the scene with one eye, in a fixed position, one could trace the scene directly onto the veil. Figure 7.2 shows this method, with a peephole to maintain a fixed eye position, as depicted by Dürer (1525).



Figure 7.2: Dürer's depiction of Alberti's veil

Alberti's veil was fine for painting actual scenes, but to paint an imaginary scene in perspective some theory was required. The basic principles Renaissance artists used were the following:

- (i) A straight line in perspective remains straight.
- (ii) Parallel lines either remain parallel or converge to a single point (their *vanishing point*).

These principles suffice to solve a problem artists frequently encountered: the perspective depiction of a square-tiled floor. Alberti (1436) solved the special case of this problem in which one set of floor lines is horizontal, that is, parallel to the horizon. Alberti's method is shown in simplified form in Figure 7.3. The receding floor lines begin at points equally spaced along the base line (imagined to touch the floor) and end at a vanishing point on the horizon. The horizontal floor lines are then determined by choosing one of them arbitrarily, thus determining one tile in the floor, and then producing the diagonal of this tile to the horizon. The intersections of this diagonal with the receding lines are the points through which the

horizontal lines pass. This is certainly true on the actual floor (Figure 7.4); hence it remains true in the perspective view.

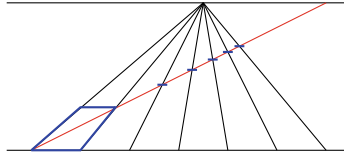


Figure 7.3: Alberti's method

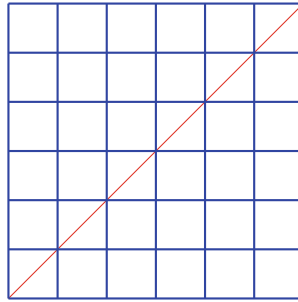


Figure 7.4: The actual floor

EXERCISES

In almost all paintings of tiled floors, one set of lines is parallel to the horizon. However, the principles (i) and (ii) suffice to generate a perspective view of a tiled floor given an arbitrarily situated tile, and they show that no measurement is needed to achieve correct spacing along the base line in Alberti's method.

- 7.1.1** Use the lines shown in Figure 7.5 to determine all lines in a pavement generated by the given tile one by one. (Hint: All the diagonals are parallel.)

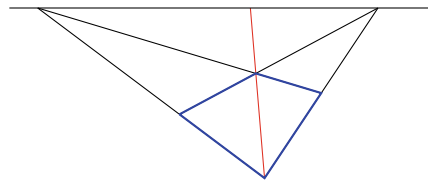


Figure 7.5: Tiled floor with arbitrary orientation

- 7.1.2** By using diagonals as in Exercise 7.1.1, show how to generate the lines in the tiling when the baseline is parallel to the horizon, without making any measurements.

7.2 Anamorphosis

It is clear from the Alberti veil construction that a perspective view will not look absolutely correct except when seen from the artist's viewpoint. Experience shows, however, that distortion is not noticeable except from extreme viewing positions. Following the mastery of perspective by the Italian artists, an interesting variation developed, in which the picture looks right from only one, extreme, viewpoint. The first known example of this style, known as *anamorphosis*, is an undated drawing by Leonardo da Vinci from the *Codex Atlanticus* (compiled between 1483 and 1518). Figure 7.6 shows part of this drawing, a child's face which looks correct when viewed with the eye near the right-hand edge of the page.



Figure 7.6: Leonardo's drawing of a face

The idea was taken up by German artists around 1530, famously in Holbein's painting *The Two Ambassadors* from 1533. A mysterious streak across the bottom of the picture becomes a skull when viewed from near the picture's edge (Figure 7.7). For more on history of anamorphosis, see Baltrušaitis (1977) and Wright (1983), pp. 146–156. The art of anamorphosis reached its technically most advanced form in France in the early 17th century. It seems no coincidence that this was also the time and place of the birth of projective geometry. In fact, key figures in the two fields, Nicéron and Desargues, were well aware of each other's work.

Nicéron (1613–1646) was a student of Mersenne and, like him, a monk in the order of Minims. He executed some extraordinary anamorphic wall paintings, up to 55 meters long, and also explained the theory in *La perspective curieuse* (1638). Figure 7.8 is his illustration of anamorphosis of

7.3 Desargues's Projective Geometry

The mathematical setting in which one can understand Alberti's veil is the family of lines ("light rays") through a point (the "eye"), together with a plane V (the "veil") (Figure 7.9). In this setting, the problems of perspective and anamorphosis were not very difficult, but the *concepts* were interesting and a challenge to traditional geometric thought. Contrary to Euclid, one had the following:

- (i) Points at infinity ("vanishing points") where parallels met.
- (ii) Transformations that changed lengths and angles (projections).

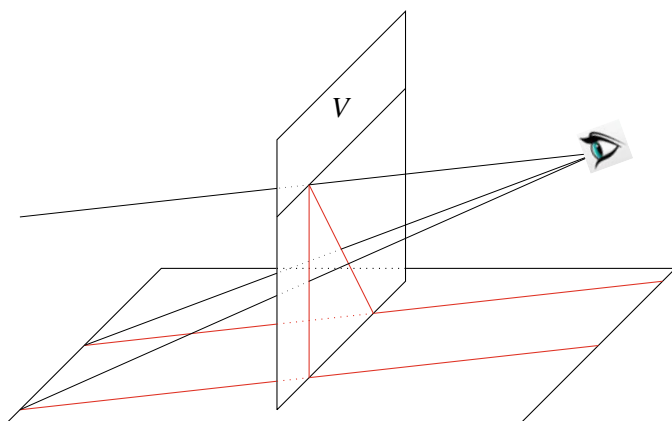


Figure 7.9: Seeing through Alberti's veil

The first to construct a mathematical theory incorporating these ideas was Desargues (1591–1661), although the idea of points at infinity had already been used by Kepler (1604), p. 93. The book of Desargues (1639), *Brouillon projet d'une atteinte aux événements des rencontres du cône avec un plan* (Schematic Sketch of What Happens When a Cone Meets a Plane), suffered an extreme case of delayed recognition, being completely lost for 200 years. Fortunately, his two most important theorems, the so-called Desargues's theorem and the invariance of the cross-ratio, were published in a book on perspective, Bosse (1648). The text of Desargues (1639) and a portion of Bosse (1648) containing Desargues's theorem may be found in Taton (1951). An English translation, with an extensive historical and mathematical analysis, is in Field and Gray (1987).

Kepler and Desargues both postulated one point at infinity on each line, closing the line to a “circle of infinite radius.” All the lines in a family of parallels share the same point at infinity. Nonparallel lines, having a finite point in common, do not have the same point at infinity. Thus any two distinct lines have exactly one point in common—a simpler axiom than Euclid’s. Strangely enough, the line at infinity was only introduced into the theory by Poncelet (1822), even though it is the most obvious line in perspective drawing, the horizon. Desargues made extensive use of projections in the *Brouillon projet*; he was the first to use them to prove theorems about conic sections.

Desargues’s theorem is a property of triangles in perspective illustrated by Figure 7.10. The theorem states that the points X , Y , Z at the intersections of corresponding sides lie on a line. This is obvious if the triangles are in space, since the line is the intersection of the planes containing them. The theorem in the plane is subtly but fundamentally different and requires a separate proof, as Desargues realized. In fact, Desargues’s theorem was shown to play a key role in the foundations of projective geometry by Hilbert (1899).

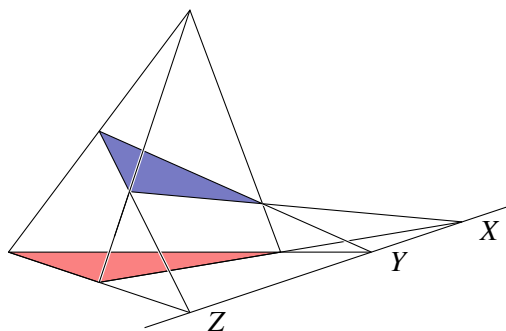


Figure 7.10: Desargues’s theorem

The second theorem of Desargues, invariance of the cross-ratio, was already known to the Greek mathematician Pappus, around 300 CE. It is Proposition 129 in his *Collection* Book VII, available in English translation in Pappus (1986). The theorem was rediscovered by Desargues and it answers a natural question about perspective raised by Alberti: since length and angle are not preserved by projection, what is?

No property of three points on a line can be invariant because any three points on a line can be projected to any three others (Exercise 7.3.1).

At least four points are therefore needed, and the cross-ratio is indeed a projective invariant of four points. If A, B, C, D are four points on a line (in that order) then their cross-ratio $(ABCD)$ is $\frac{CA}{CB} / \frac{DA}{DB}$. Its invariance is most simply seen by reexpressing it in terms of angles using Figure 7.11.

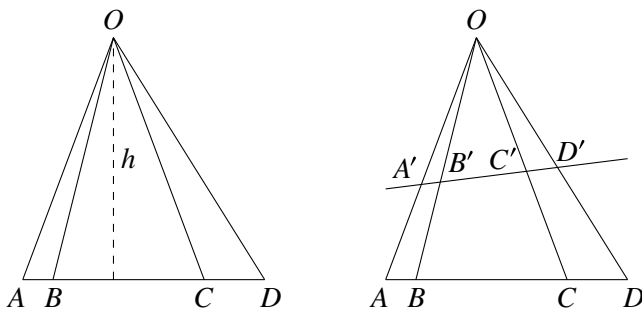


Figure 7.11: Evaluating the cross-ratio

Let O be any point outside the line and consider the areas of the triangles OCA , OCB , ODA , and ODB . First compute them from bases on AB and height h , then recompute using OA and OB as bases and heights expressed in terms of the sines of angles at O :

$$\begin{aligned} \frac{1}{2}h \cdot CA &= \text{area } OCA = \frac{1}{2}OA \cdot OC \sin \angle COA, \\ \frac{1}{2}h \cdot CB &= \text{area } OCB = \frac{1}{2}OB \cdot OC \sin \angle COB, \\ \frac{1}{2}h \cdot DA &= \text{area } ODA = \frac{1}{2}OA \cdot OD \sin \angle DOA, \\ \frac{1}{2}h \cdot DB &= \text{area } ODB = \frac{1}{2}OB \cdot OD \sin \angle DOB. \end{aligned}$$

Substituting the values of CA , CB , DA , and DB from these equations we find, following Möbius (1827), the cross-ratio in terms of angles at O :

$$\frac{CA}{CB} \Big/ \frac{DA}{DB} = \frac{\sin \angle COA}{\sin \angle COB} \Big/ \frac{\sin \angle DOA}{\sin \angle DOB}.$$

Any four points A', B', C', D' in perspective with A, B, C, D from a point O have the same angles (Figure 7.11); hence they will have the same cross-ratio. But then so will any four points A'', B'', C'', D'' projectively related to A, B, C, D , since a projectivity is by definition the product of a sequence of perspectivities.

EXERCISES

As mentioned above, we cannot hope for an invariant that is simpler than the cross-ratio, because any three points in a line are projectively related to any other.

7.3.1 Show that any three points on a line can be sent to any other three points on a line by projection. (You may move the lines to a convenient position.)

7.4 The Projective View of Curves

The first works in projective geometry, by Desargues (1639) and Pascal (1640), used the language of classical geometry, even though the language of equations was available from Descartes (1637). At that time the advantages of the projective method were more clearly seen in a classical setting. Desargues and Pascal confined themselves to straight lines and conic sections, showing how projective geometry could easily reach and surpass the results obtained by the Greeks. Moreover, the projective viewpoint gave something else that would have been incomprehensible to the Greeks: a clear account of the behavior of curves at infinity.

For example, Desargues (1639) (in Taton (1951), p. 137) distinguished the ellipse, parabola, and hyperbola by their numbers of points at infinity: 0, 1, and 2, respectively. The points at infinity on the parabola and hyperbola can be seen quite plainly by tilting the ordinary views of them into perspective views (Figures 7.12 and 7.13). The parabola has just one point at infinity because it crosses each ray through 0, except the y -axis, at one other point.

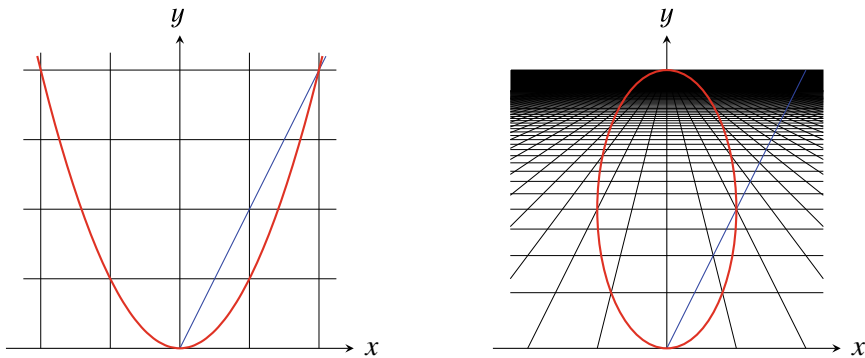


Figure 7.12: The parabola: direct and perspective view

As for the hyperbola, its two points at infinity are where it touches its asymptotes, as seen in Figure 7.13. The continuation of the hyperbola above the horizon results from projecting the lower branch through the same center of projection (Figure 7.14).

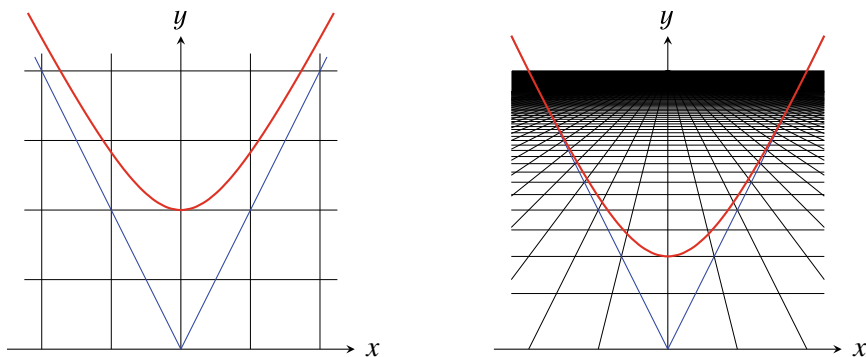


Figure 7.13: The hyperbola: direct and perspective view

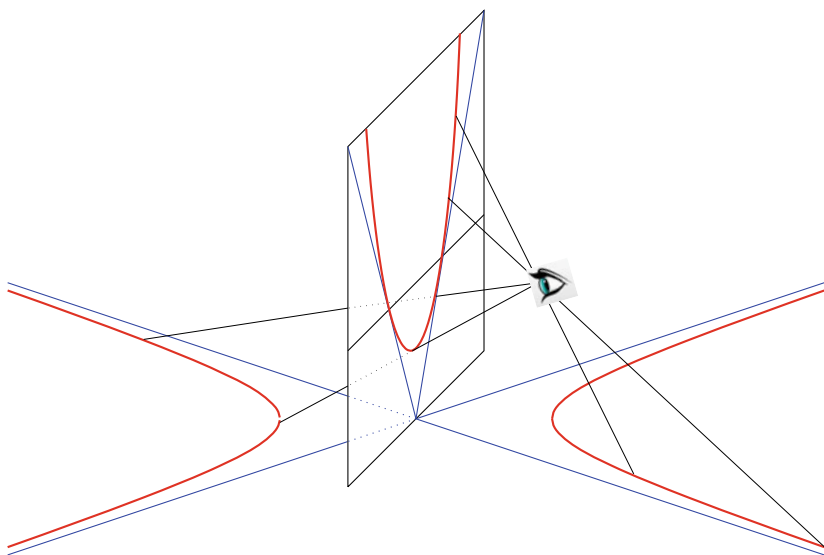


Figure 7.14: Branches of the hyperbola

Projective geometry goes beyond describing the behavior of curves at infinity. The line at infinity is no different from any other line and can

be deprived of its special status. Then all projective views of a curve are equally valid and one can say, for example, that all conic sections are ellipses when suitably viewed. This is no surprise if one thinks of conic sections not as second-degree curves but as sections of the cone. Of course they all look the same from the vertex of the cone!

Cubic Curves

More surprisingly, a great simplification of cubic curves also occurs when they are viewed projectively. As mentioned in Section 6.4, Newton (1695) classified cubic curves into 72 types (and missed 6). However, in his Section 29, “On the Genesis of Curves by Shadows,” Newton claimed that each cubic curve can be projected onto one of just five types. As mentioned in Section 6.4, this includes the result that $y = x^3$ can be projected onto $y^2 = x^3$. The proof of this is an easy calculation when coordinates are introduced (see Exercise 7.7.2), but one already gets an inkling of it from the perspective view of $y = x^3$. See Figure 7.15. The lower half of the cusp is the view of $y = x^3$ below the horizon; the upper half comes from projecting the view behind one’s head through the eye to the picture plane in front.

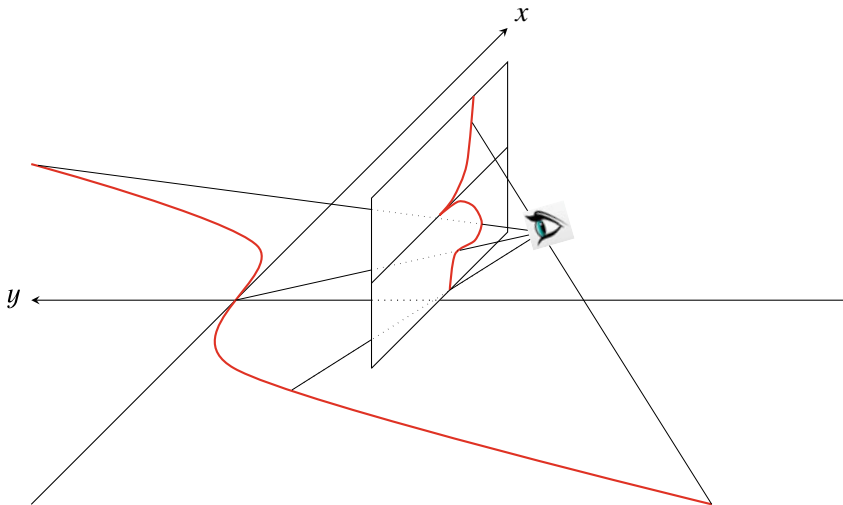


Figure 7.15: Perspective view of $y = x^3$

Conversely, $y^2 = x^3$ has an inflection at infinity. Newton’s projective classification comes from studying the behavior at infinity of all cubics and

observing that each has characteristics already possessed, not necessarily at infinity, by curves of the form

$$y^2 = Ax^3 + Bx^2 + Cx + D.$$

Newton had already divided these into five types in his analytic classification. They are the five shown in Figure 6.3. Newton's result was improved only in the 19th century, when projective classification over the complex numbers reduced the number of types of cubics to just three. We discuss this later in connection with complex numbers (Section 12.5).

EXERCISES

As suggested above, the points at infinity of a curve may be counted by considering intersections of the curve with lines through the origin, and observing where they tend to infinity.

7.4.1 Use this method to explain why

- the hyperbola $xy = 1$ has two points at infinity,
- the curve $y = x^3$ has one point at infinity.

Figures 7.12 and 7.13 were made by taking Alberti's veil to be the (x, z) -plane in (x, y, z) -space, with the "eye" at $(0, -4, 4)$ viewing the (x, y) -plane tiled with unit squares.

7.4.2 Find the parametric equations of the line from $(0, -4, 4)$ to $(x', y', 0)$, and hence show that this line meets the veil where

$$x = \frac{4x'}{y' + 4}, \quad z = \frac{4y'}{y' + 4}.$$

7.4.3 Renaming the coordinates x, z in the veil as X, Y respectively, show that

$$x' = \frac{4X}{4 - Y}, \quad y' = \frac{4Y}{4 - Y}.$$

7.4.4 Deduce from Exercise 7.4.3 that the points (x', y') on the parabola $y = x^2$ have image on the veil

$$X^2 + \frac{(Y - 2)^2}{4} = 1,$$

and check that this is the ellipse shown in Figure 7.12.

7.5 The Projective Plane

The way projective geometry puts infinity on the same footing as the finite points of the plane is intuitively clear when one thinks of the horizon in a picture, which is a line like any other. But what, mathematically speaking, is this line we see? To model the situation we take the plane in view to be the plane $z = -1$ in the three-dimensional space with coordinates (x, y, z) , and place our eye at the origin $O = (0, 0, 0)$, as in Figure 7.16.

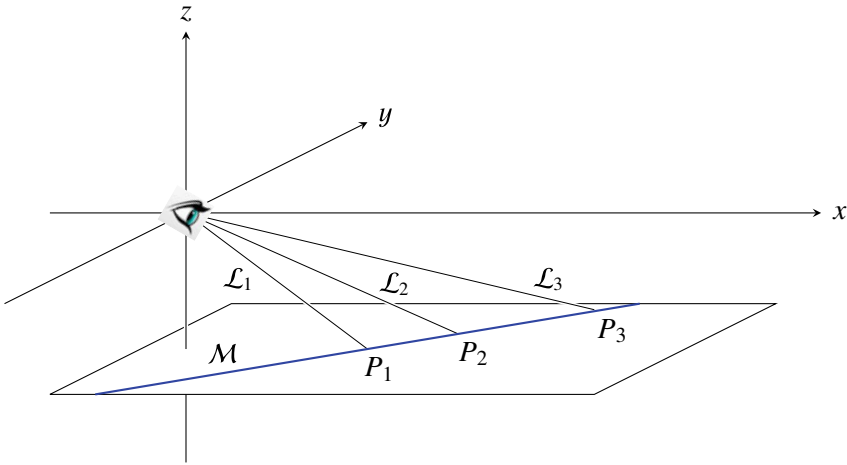


Figure 7.16: Viewing the plane

Points P_1, P_2, P_3, \dots in the plane lie on “lines of sight” $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3, \dots$ through O , and as the point P_n tends to infinity its line of sight \mathcal{L}_n tends to horizontal. Therefore, it is natural to interpret each horizontal line through O , which does not correspond to an actual point of the plane, as the line of sight to a “point at infinity” of the plane. More boldly, we can define the lines through O to be the points of a *projective plane*, called the *real projective plane* \mathbb{RP}^2 , and the planes through O to be the lines of \mathbb{RP}^2 —the so-called *projective lines*.

Modeling the points of the plane $z = -1$ by the non-horizontal lines through O enables us to *complete* this ordinary plane to a projective plane by using the remaining lines through O (which are not called “horizontal” for nothing!) to model the points on its horizon. Moreover, the horizontal plane through O models the horizon line, reinforcing our intuition that the horizon is a line like any other.

This model of the projective plane is geometrically as natural as one could wish, and it answers certain questions that are confusing for vision alone. For example, we can see why it is proper for a line M in the ordinary plane to have only one point at infinity: because there is only *one* line through O to which the lines through P_1, P_2, P_3, \dots tend as P_n tends to infinity, namely, the parallel to M through O . Thus, Kepler and Desargues were not far wrong in thinking of a projective line as a circle. The two “ends” of the line are joined by its single point at infinity.

While a projective line is essentially a circle, a projective plane is *not* essentially a sphere, but something more peculiar, as was noticed by Klein (1874). \mathbb{RP}^2 is essentially a *sphere with antipodal points identified*, where antipodal points P, P' are pairs such as those shown in Figure 7.17: the diametrically opposite points at which a line through O meets the unit sphere with center O . “Identifying” the points P, P' means treating the pair (P, P') as a single point. This is appropriate since the pair corresponds to a single line through O , that is, to a single point of \mathbb{RP}^2 .

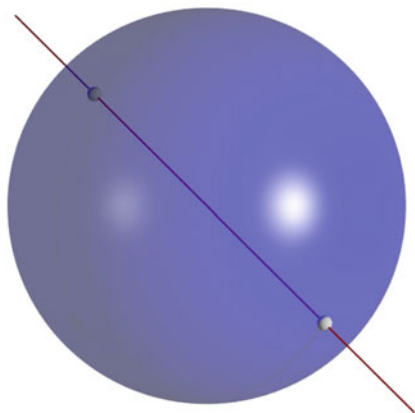


Figure 7.17: Antipodal point pair

The surface \mathbb{RP}^2 modeled by the pairs (P, P') is strikingly different from the sphere of individual points P . For example, on a sphere, any simple closed curve separates the surface into two parts. A “small” closed curve in \mathbb{RP}^2 —that is, one strictly contained in a hemisphere of the model—also separates it, but a “large” one may not. The equator, for instance,

does not separate the upper hemisphere from the lower, because the hemispheres are the *same place* under antipodal point identification! A less paradoxical view of this is seen by going back to the model of \mathbb{RP}^2 whose elements are lines through O . The lines through the equator do not separate the lines through the upper hemisphere from the lines through the lower hemisphere, because these are the same lines.

EXERCISES

The model of the projective plane whose points are lines through O and whose lines are planes through O also helps in visualizing other basic properties of projective lines.

7.5.1 Use this interpretation of projective lines to show that all lines in a family of parallels have the same point at infinity.

7.5.2 Likewise, show that any two projective lines meet in exactly one point.

Now let us return to the interpretation of the projective plane as a surface, the sphere with antipodal points identified. The following result shows another way in which the projective plane differs from a sphere.

7.5.3 Show that a strip of the projective plane surrounding a projective line is a Möbius band (Figure 7.18).

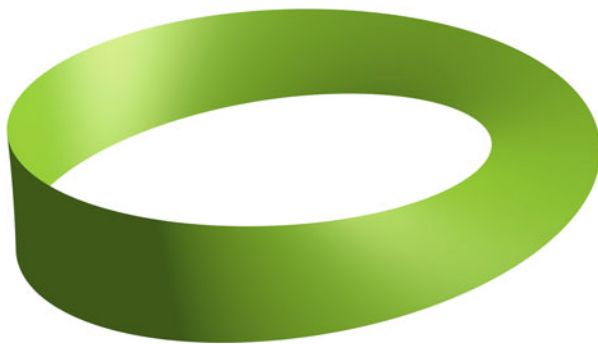


Figure 7.18: A Möbius band

7.5.4 Why is the Möbius band not a part of the sphere?

7.6 The Projective Line

As we have seen, projective geometry arose from efforts to understand the relationship between two and three dimensions. But the idea arising from these efforts—that of *projection* or *projective transformations*—is interesting even in one dimension. In this section we make a more detailed study of projection from a line to a line, and use it to present a more sophisticated concept of projective line. In the process, we meet the concept of *linear fractional transformation*, which plays a key role in many later developments. In particular, we will show how linear fractional transformations give a new insight into the invariance of the cross-ratio.

We start by viewing the line as the number line \mathbb{R} , and study how the numerical values of points are related when we project one line onto another. The simplest kind of projection is *parallel projection* (or projection from infinity) of a line onto a parallel line, as shown in Figure 7.19.

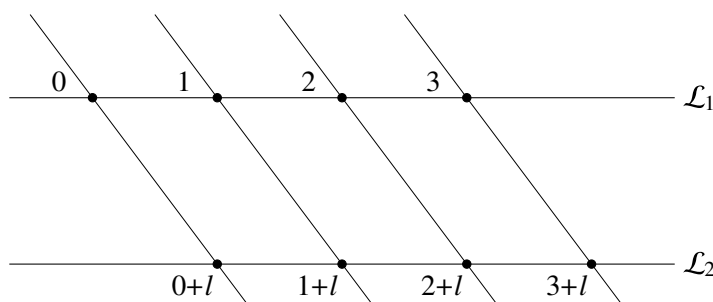


Figure 7.19: Projection from infinity

Clearly, when we make the natural choice of coordinates on the two lines, parallel projection sends x on \mathcal{L}_1 to $x + l$ on \mathcal{L}_2 , for some constant l . We abbreviate this mapping of coordinates by $x \mapsto x + l$.

If we project from a point P at a finite distance, then it is likewise clear from Figure 7.20 (where we align the zero point on each line with P) that x on \mathcal{L}_1 is sent to kx on \mathcal{L}_2 for some nonzero constant k . We abbreviate this mapping of coordinates by $x \mapsto kx$ ($k \neq 0$).

A more remarkable case is shown in Figure 7.21, where we project a line \mathcal{L}_1 onto a perpendicular line \mathcal{L}_2 from a point not on either line, but equidistant from both. Then, with suitable choice of coordinates, x on \mathcal{L}_1 is sent to $1/x$ on \mathcal{L}_2 .

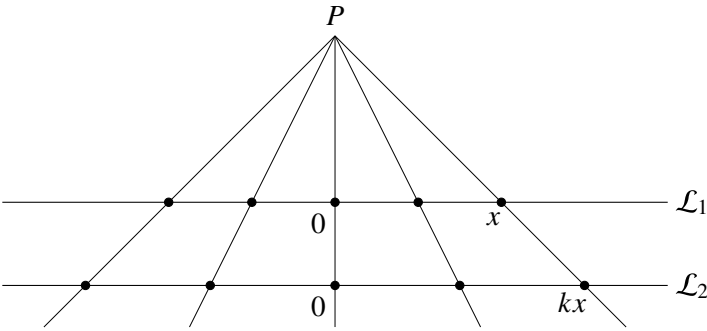


Figure 7.20: Projection from a finite point

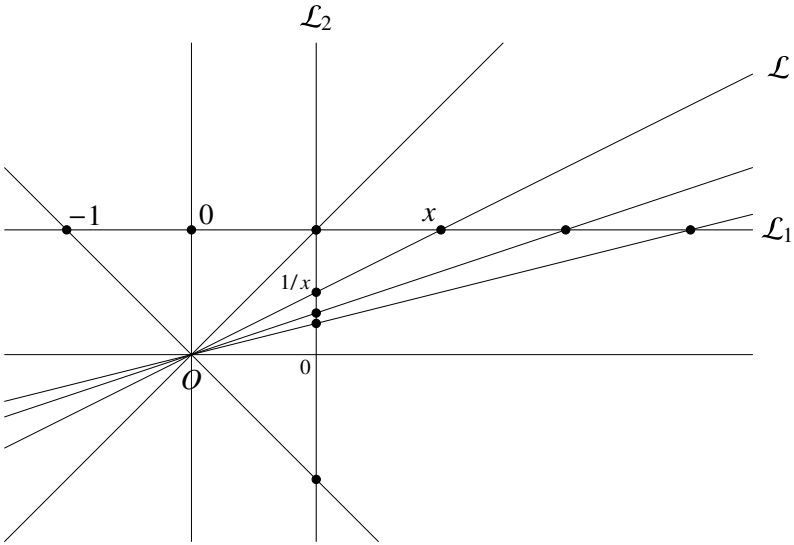


Figure 7.21: Projection of a line onto a perpendicular line

This makes \mathcal{L}_2 a highly distorted image of \mathcal{L}_1 , with the equally spaced points $1, 2, 3, 4, \dots$ on \mathcal{L}_1 going to the points $1, 1/2, 1/3, 1/4, \dots$ on \mathcal{L}_2 . These image points tend to the point 0 on \mathcal{L}_2 , which is *not* the projection of any point on \mathcal{L}_1 . However, if we extend \mathcal{L}_1 by an extra point ∞ —its point at infinity—then it seems right to view 0 on \mathcal{L}_2 as the projection of ∞ on the extended line $\mathcal{L}_1 \cup \{\infty\}$. It likewise seems right to extend \mathcal{L}_2 by its point ∞ at infinity, and to view this point as the projection of 0 on \mathcal{L}_1 .

If we still claim that this map sends x to $1/x$, then we must admit that

$$1/0 = \infty \quad \text{and} \quad 1/\infty = 0.$$

We have legalized division by zero! Is this valid? In this limited setting, yes. Each line \mathcal{L} through O is marked with two symbols: x and $1/x$. If \mathcal{L} is neither vertical nor horizontal, then x and $1/x$ are the intersections of \mathcal{L} with \mathcal{L}_1 and \mathcal{L}_2 respectively; if \mathcal{L} is vertical, then $x = 0$ is its real intersection with \mathcal{L}_1 and $1/0 = \infty$ is its “intersection at infinity” with its parallel \mathcal{L}_2 ; if \mathcal{L} is horizontal, then $1/x = 1/\infty = 0$ is its real intersection with \mathcal{L}_2 and ∞ is its “intersection at infinity” with its parallel \mathcal{L}_1 .

Actually, division by zero is valid in the more general and interesting setting of linear fractional transformations:

$$f(x) = \frac{ax + b}{cx + d}, \quad \text{where} \quad ad - bc \neq 0.$$

These are precisely the functions obtainable as combinations of the functions $x \mapsto x + l$, $x \mapsto kx$ for $k \neq 0$, and $x \mapsto 1/x$, and they correspond to arbitrary projections of one projective line onto another. To be precise, each linear fractional function gives a well-defined and one-to-one map of $\mathbb{R} \cup \{\infty\}$ to itself, and these maps realize all projections of the projective line. See the exercises below. Because of this, we call $\mathbb{R} \cup \{\infty\}$, together with its linear fractional functions, the *real projective line* \mathbb{RP}^1 .

The linear fractional functions give \mathbb{RP}^1 its “projective” nature. \mathbb{RP}^1 has no concept of length, because length is not preserved by linear fractional functions. Not even the ratio of lengths is preserved, as one can see with the function $x \mapsto 1/x$. However, *the cross-ratio is preserved by linear fractional functions*, and hence by projections.

To see why, consider four points A, B, C, D on a line. If we view these points as numbers, then their cross-ratio (defined in Section 7.3) becomes

$$\frac{CA \cdot DB}{CB \cdot DA} = \frac{(C - A)(D - B)}{(C - B)(D - A)}.$$

The function $x \mapsto x + l$, which adds l to each of A, B, C, D , obviously does not change the cross-ratio. Neither does the function $x \mapsto kx$ for $k \neq 0$, which multiplies each of A, B, C, D by k . It is less obvious that the cross-ratio is preserved by the function $x \mapsto 1/x$, but a simple calculation confirms this. Thus the cross-ratio is preserved by all combinations of $x \mapsto x + l$, $x \mapsto kx$ for $k \neq 0$, and hence by all linear fractional functions.

EXERCISES

We can see why each linear fractional function is a combination of functions of the forms $x \mapsto x + l$, $x \mapsto kx$ for $k \neq 0$, and $x \mapsto 1/x$ by a suitable breakdown of the fraction $\frac{ax+b}{cx+d}$.

7.6.1 Show that $\frac{ax+b}{cx+d} = \frac{a}{c} + \frac{bc-ad}{c(cx+d)}$ if $c \neq 0$.

7.6.2 Deduce from Exercise 7.6.1 that the function $x \mapsto \frac{ax+b}{cx+d}$ is a combination of functions $x \mapsto x + l$, $x \mapsto kx$, and $x \mapsto 1/x$ when $c \neq 0$. What if $c = 0$?

7.6.3 What property of $\frac{ax+b}{cx+d}$ is controlled by the condition $ad - bc \neq 0$?

7.6.4 Verify that the cross-ratio $\frac{(C-A)(D-B)}{(C-B)(D-A)}$ remains unchanged when each of the points A, B, C, D is replaced by its reciprocal.

It follows that the cross-ratio is preserved by any linear fractional function. It remains to show that projections are realized by linear fractional functions. We have already done this for projection of a line onto a parallel line. Hence it remains to study projection of a line, say the x -axis, onto a line that intersects it, say $y = cx$.

7.6.5 Show that projection from the point (a, b) sends the point $x = t$ on the x -axis to the point on the line $y = cx$ for which

$$x = \frac{bt}{ct + b - ca},$$

which is a linear fractional function of t .

7.7 Homogeneous Coordinates

Representing the points of the projective plane \mathbb{RP}^2 by lines through O gives *coordinates* to \mathbb{RP}^2 via the coordinates (x, y, z) of three-dimensional space. Such coordinates were invented by Möbius (1827) and Plücker (1830), and they are called *homogeneous* because each algebraic curve in \mathbb{RP}^2 is expressed by a homogeneous polynomial equation $p(x, y, z) = 0$. The simplest case is that of a projective line, which, as we saw in Section 7.5, is represented by a plane through O . Its equation therefore has the form

$$ax + by + cz = 0, \quad \text{for some constants } a, b, c, \text{ not all zero.}$$

Such an equation is called *homogeneous of degree 1*, because each nonzero term is of degree 1 in the variables x, y, z .

The *homogeneous coordinates of a point P* in \mathbb{RP}^2 are simply the coordinates of *all* points on the line through O that represents P . It follows that

if (x, y, z) is one coordinate triple for P , so is (tx, ty, tz) for any real number t . And if $p(x, y, z) = 0$ is the equation of a curve in \mathbb{RP}^2 , the polynomial p must be such that

$$p(tx, ty, tz) = 0 \quad \text{for all real numbers } t.$$

It follows that $p(tx, ty, tz) = t^n p(x, y, z)$ for some n , called the *degree* of p .

A typical example is the equation

$$x^2 - yz = 0,$$

which is homogeneous of degree 2. To see what this curve looks like in an ordinary plane, such as $z = 1$, we substitute for the appropriate variable. With $z = 1$ we obtain

$$y = x^2,$$

which is the equation of a parabola in the plane $z = 1$. Thus $x^2 - yz = 0$ is the *projective completion* of a parabola, with a point at infinity added (namely, the y -axis, where $x = z = 0$).

But $x^2 - yz = 0$ is also the projective completion of a hyperbola. We see this by intersecting the projective curve with the plane $x = 1$, obtaining the hyperbola $yz = 1$. Surprising as this seems at first, it reflects a fact we already know from Section 7.4—that all conic sections are projectively the same.

Homogeneous coordinates also make it easy to show that certain cubic curves have the same projective completion (see Exercise 7.7.2).

Bézout's Theorem Revisited

As we saw in Section 6.5, to obtain Bézout's theorem that a curve of degree m meets a curve of degree n in mn points we need a precise account of points at infinity. Homogeneous coordinates simplify this problem by changing it to one about homogeneous polynomials. If C_m is a curve with homogeneous equation of degree m ,

$$p_m(x, y, z) = 0, \tag{1}$$

and if C_n is a curve with homogeneous equation of degree n ,

$$p_n(x, y, z) = 0, \tag{2}$$

one wishes to show that the equation

$$r_{mn}(x, y) = 0, \quad (3)$$

which results from eliminating z between (1) and (2), is homogeneous of degree mn . This is not hard to do (see exercises), but it seems that a homogeneous formulation of Bézout's theorem, with a rigorous proof that the resultant r_{mn} has degree mn , was not given until the late 1800s. According to Kline (1972), p. 553, the "proper count of multiplicities" was first made by Halphen in 1873.

An obvious condition must be included in the hypothesis of Bézout's theorem: that the curves C_m and C_n have no common component. The algebraic equivalent of this condition is that the polynomials p_m, p_n have no nonconstant common factor. Then the form of Bézout's theorem that can be proved with the help of homogeneous coordinates is *curves C_m, C_n with homogeneous equations $p_m(x, y, z) = 0, p_n(x, y, z) = 0$ of degrees m, n and no common component have intersections given by the solutions of a homogeneous equation $r_{mn}(x, y) = 0$ of degree mn .*

EXERCISES

7.7.1 We know that the hyperbola $yz = 1$ has two points at infinity. To which lines through O do they correspond in the projective completion $x^2 - yz = 0$?

7.7.2 By considering the homogeneous polynomial equation $x^3 - y^2z = 0$, show that the cubic curves $y = x^3$ and $y^2 = x^3$ have the same projective completion.

As the Chinese discovered (see Section 5.2), the problem of elimination belongs to linear algebra. In the case of Bézout's theorem, this includes the criterion that determinant $= 0$ for a set of homogeneous equations to have a nonzero solution, and it leads to an expression for the resultant r_{mn} as a determinant.

7.7.3 Suppose that

$$\begin{aligned} p_m(x, y, z) &= a_0z^m + a_1z^{m-1} + \cdots + a_m, \\ p_n(x, y, z) &= b_0z^n + b_1z^{n-1} + \cdots + b_n \end{aligned}$$

are homogeneous polynomials of degrees m, n . Thus $a_i(x, y)$ is homogeneous of degree i and $b_j(x, y)$ is homogeneous of degree j . By multiplying p_m and p_n by suitable powers of z , show that the equations

$$p_m = 0 \quad \text{and} \quad p_n = 0$$

are equivalent to a system of $m + n$ homogeneous linear equations in the variables $z^{m+n-1}, \dots, z^2, z^1, z^0$, which in turn is equivalent to

$$r_{mn}(x, y) \equiv \begin{vmatrix} a_0 & a_1 & \cdots & a_m & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_m & 0 & \cdots & 0 \\ \vdots & & \ddots & & & \ddots & \ddots & \\ 0 & \cdots & 0 & a_0 & & \cdots & & a_m \\ b_0 & b_1 & \cdots & & b_n & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & & b_n & & \vdots \\ \vdots & & \ddots & & & & \ddots & 0 \\ 0 & \cdots & 0 & b_0 & & \cdots & & b_n \end{vmatrix} = 0.$$

7.7.4 Show that a polynomial $p(x, y)$ is homogeneous of degree $k \Leftrightarrow p(tx, ty) = t^k p(x, y)$.

7.7.5 Show that $r_{mn}(tx, ty) = t^{mn} r_{mn}(x, y)$. *Hint:* Multiply the rows of $r_{mn}(tx, ty)$ by suitable powers of t to arrange that each element in any column contains the same power of t . Then remove these factors from the columns so that $r_{mn}(x, y)$ remains.



8

Calculus

PREVIEW

The shift towards algebraic thinking was not only a revolution in geometry. It was decisive in the second and greatest mathematical revolution of the 17th century: the invention of calculus. It is true that some results we now obtain by calculus were known to the ancients; for example, the area of the parabolic segment was found by Archimedes. But the *systematic computation* of areas, volumes, and tangents became possible only when symbolic computation—that is, algebra—became available.

The dependence of calculus on algebra is particularly clear in the work of Newton, whose calculus is essentially the algebra of infinite polynomials (power series). Moreover, Newton's starting point was a basic theorem about the polynomial $(1 + x)^n$, the *binomial theorem*, which he extended to fractional values of n .

The calculus of Leibniz was likewise based on algebra—in his case the algebra of *infinitesimals*. Despite doubts about the meaning and existence of infinitesimals, Leibniz and his followers obtained correct results by computing with them.

Results that we now obtain through a combination of algebra and limit processes were obtained by Leibniz through the algebra of infinitesimals. Our *derivative* dy/dx was, for Leibniz, literally the quotient of the infinitesimal dx by the infinitesimal dy . And our *integral* $\int f(x) dx$ was, for Leibniz, literally the sum of the infinitesimals $f(x) dx$ (hence the symbol \int , which is an elongated S for “sum”).

8.1 What Is Calculus?

Calculus emerged in the 17th century as a system of shortcuts to results obtained by the method of exhaustion and as a method for discovering such results. The types of problem suited to calculus were finding lengths, areas, and volumes of curved figures and determining local properties such as tangents, normals, and curvature—in short, what we now recognize as problems of integration and differentiation. Equivalent problems of course arise in mechanics, where one of the dimensions is time instead of distance; hence calculus also made mathematical physics possible. In addition, calculus was intimately connected with the theory of infinite series, initiating developments that became fundamental in number theory, combinatorics, and probability theory.

The extraordinary success of calculus was possible, in the first instance, because it replaced long and subtle exhaustion arguments by short routine calculations. As the name suggests, calculus consists of *rules for calculating* results, not their logical justification. Mathematicians of the 17th century were familiar with the method of exhaustion and assumed they could always fall back on it if their results were challenged, but the flood of new results became so great that there was seldom time to do so. As Huygens (1659), p. 337, wrote,

Mathematicians will never have enough time to read all the discoveries in Geometry (a quantity which is increasing from day to day and seems likely in this scientific age to develop to enormous proportions) if they continue to be presented in a rigorous form according to the manner of the ancients.

The progress in geometry when Huygens wrote was indeed impressive, considering the very simple system of calculus then available. Virtually all that was known was the differentiation and integration of powers of x (possibly fractional) and implicit differentiation of polynomials in x and y . However, when allied with algebra and analytic geometry, this was sufficient to find tangents, maxima, and minima for all algebraic curves. And when allied with Newton's calculus of infinite series, discovered in the 1660s, the rules for powers of x formed a complete system for differentiation and integration of all functions expressible in power series.

The subsequent development of calculus is a puzzling exception to the normal process of simplification in mathematics. Nowadays we have a

much less elegant system, which downplays the use of infinite series and complicates the system of rules for differentiation and integration. The rules for differentiation are still complete, given a sensible set of operations for constructing functions, but the rules for integration are pathetically incomplete. They do not suffice to integrate simple algebraic functions like $\sqrt{1+x^3}$, or even rational functions with undetermined constants like $1/(x^5 - x - A)$. Moreover, it is only in recent decades that we have been able to tell *which* algebraic functions are integrable by our rules. (This little-known result is expounded by Davenport (1981).)

The conclusion seems to be that, apart from streamlining the language slightly, we cannot make calculus any simpler than it was in the 17th century! It is certainly easier to present the history of the subject if we refrain from imposing modern ideas. This approach also has the advantage of emphasizing the computational nature of calculus—it is about *calculation*, after all.

Much has been written on the history of calculus, and some useful books are Boyer (1959), Baron (1969), Edwards (1979), and Bressoud (2019). The earlier historians are inclined to harp on the question of logical justification and to spend a disproportionate amount of time on the way it was handled in the 19th century. This tends to obscure the boldness and vigor of early calculus, and can be dogmatic about the way in which calculus should be justified. Apart from the justification already available in the 17th century (the method of exhaustion), there is also a 20th-century justification (the new theory of infinitesimals of Robinson (1966)). The sheer diversity of foundations for calculus suggests that we have not yet got to the bottom of it.

8.2 Early Results on Areas and Volumes

The idea of integration is often introduced by approximating the area under curves $y = x^k$ by rectangles (Figure 8.1), say, from 0 to 1. If the base of the region is divided into n equal parts, then the heights of the rectangles are $(1/n)^k, (2/n)^k, \dots, (n/n)^k$, and the area occupied by the rectangles depends on the series $1^k + 2^k + \dots + n^k$. If the curve is revolved around the x -axis, then the rectangles sweep out cylinders of cross-sectional area πr^2 , where $r = (1/n)^k, (2/n)^k, \dots, (n/n)^k$, whose sum depends on $1^{2k} + 2^{2k} + \dots + n^{2k}$.

After the time of Archimedes, the first new results on areas and volumes were in fact based on summing these series. The Arab mathematician

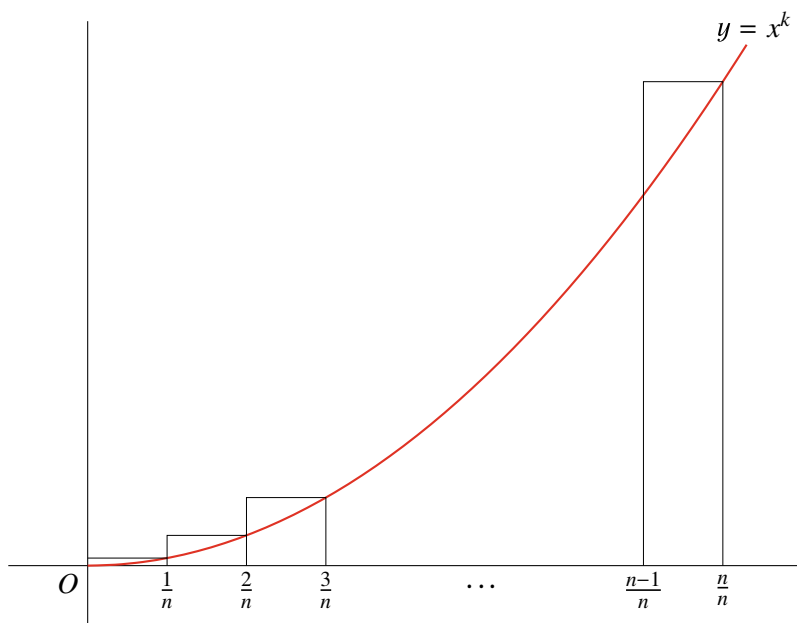


Figure 8.1: Approximating an area by rectangles

al-Haytham (around 965–1039) summed the series $1^k + 2^k + \cdots + n^k$ for $k = 1, 2, 3, 4$, and used the result to find the volume of the solid obtained by rotating the parabola about its base. See Baron (1969), p. 70, or Edwards (1979), p. 84, for al-Haytham’s method.

Cavalieri (1635) extended these results up to $k = 9$, using them to obtain the equivalent of

$$\int_0^a x^k dx = \frac{a^{k+1}}{k+1}$$

and conjecturing this formula for all positive integers k . This result was proved in the 1630s by Fermat, Descartes, and Roberval. Fermat even obtained the result for fractional k (see Baron (1969), pp. 129, 185, and Edwards (1979), p. 116). Cavalieri is best known for his *method of indivisibles*, an early method of discovery that divided areas into infinitely thin strips and volumes into infinitely thin slices. Archimedes’ *Method* used similar ideas but, as mentioned in Section 4.1, this was not known until the 20th century. Remarkably, Cavalieri’s contemporary Torricelli (the inventor of the barometer) speculated that such a method may have been

used by the Greeks. One of Torricelli's own discoveries, which caused astonishment at the time, was that the infinite solid obtained by revolving $y = 1/x$ about the x axis from 1 to ∞ has finite volume (Torricelli (1643) and Exercise 8.2.3). The philosopher Hobbes (1672) wrote of Torricelli's result that "to understand this for sense, it is not required that a man should be a geometrician or logician, but that he should be mad."

EXERCISES

- 8.2.1** Find $1 + 2 + \cdots + n$ by summing the identity $(m + 1)^2 - m^2 = 2m + 1$ from $m = 1$ to n . Similarly find $1^2 + 2^2 + \cdots + n^2$ using the identity

$$(m + 1)^3 - m^3 = 3m^2 + 3m + 1$$

together with the previous result. Likewise, find $1^3 + 2^3 + \cdots + n^3$ using the identity

$$(m + 1)^4 - m^4 = 4m^3 + 6m^2 + 4m + 1$$

and so on.

- 8.2.2** Show that the approximation to the area under $y = x^2$ by rectangles in Figure 8.1 has value $(2n + 1)n(n + 1)/6n^3$, and deduce that the area under the curve is $1/3$.

- 8.2.3** Show that the volume of the solid obtained by rotating the portion of $y = 1/x$ from $x = 1$ to ∞ about the x -axis is finite. Show, on the other hand, that its surface area is infinite.

Cavalieri's most elegant application of his method of indivisibles was to prove Archimedes' formula for the volume of a sphere. His argument is simpler than that of Archimedes, and it goes as follows.

- 8.2.4** Show that the slice $z = c$ of the sphere $x^2 + y^2 + z^2 = 1$ has the same area as the slice $z = c$ of the cylinder $x^2 + y^2 = 1$ outside the cone $x^2 + y^2 = z^2$ (Figure 8.2).

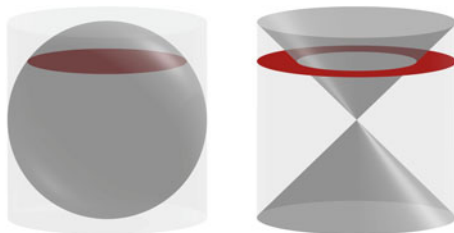


Figure 8.2: Slices considered by Cavalieri

- 8.2.5** Deduce from Exercise 8.2.4, and the known volume of the cone, that the volume of the sphere is $2/3$ the volume of the circumscribing cylinder.

8.3 Maxima, Minima, and Tangents

The idea of differentiation is now considered to be simpler than integration, but historically it developed later. Apart from the construction of the tangent to the spiral $r = a\theta$ by Archimedes, no examples of the characteristic limiting process

$$\lim_{\Delta x \rightarrow 0} \frac{f(x + \Delta x) - f(x)}{\Delta x}$$

appeared until it was introduced by Fermat in 1629 for polynomials f and used to find maxima, minima, and tangents. Fermat's work, like his discovery of analytic geometry, was not published until 1679, but it became known to other mathematicians through correspondence after a more complicated tangent method was published by Descartes (1637).

Fermat's calculations involve a sleight of hand also used by Newton and others: introduction of a "small" or "infinitesimal" element E at the beginning, dividing by E to simplify, then omitting E at the end as if it were zero. For example, to find the slope of the tangent to $y = x^2$ at any value x , consider the chord between the points (x, x^2) and $(x + E, (x + E)^2)$ on it:

$$\begin{aligned} \text{slope} &= \frac{(x + E)^2 - x^2}{E} \\ &= \frac{2xE + E^2}{E} = 2x + E. \end{aligned}$$

We now get the slope of the tangent by neglecting E . By seeming to claim that $2x + E = 2x$ and at the same time $E \neq 0$, this procedure enraged philosophers such as Hobbes. We know it is only necessary to claim that $\lim_{E \rightarrow 0}(2x + E) = 2x$, but 17th-century mathematicians did not know how to say this. In any case, they were too carried away with the power of the method to worry about such criticisms (and it was hard to take philosophers seriously when they were as obstinate as Hobbes; see previous section). Fermat's method applies to all polynomials $p(x)$, since the highest-degree term in $p(x + E)$ is always canceled by the highest-degree term in $p(x)$, leaving terms divisible by E . Fermat also extended it to curves given by polynomial equations $p(x, y) = 0$. He did this in 1638 when Descartes, hoping to stump him, proposed finding the tangent to the folium.

The generality of Fermat's method entitles him to be regarded as one of the founders of calculus. He could certainly find tangents to all curves given by polynomial equations $y = p(x)$ and probably to all algebraic curves $p(x, y) = 0$. A completely explicit rule for the latter problem was found by Sluse about 1655 (but not published until Sluse (1673)) and by Hudde in 1657 (published in the 1659 edition of Descartes's *La Géométrie*, Schooten (1659)). In our notation, if

$$p(x, y) = \sum a_{ij} x^i y^j = 0,$$

then

$$\frac{dy}{dx} = -\frac{\sum i a_{ij} x^{i-1} y^j}{\sum j a_{ij} x^i y^{j-1}}.$$

Nowadays, this result is easily obtained by implicit differentiation (see the exercises below), but it can also be obtained by direct manipulation of polynomials.

EXERCISES

For evidence that tangents to algebraic curves may be found without calculus, it is enough to look more closely at what we called Diophantus's tangent method in Section 3.5. In his *Arithmetica*, Problem 18, Book VI (previously mentioned in Exercise 3.5.1), Diophantus finds the tangent $y = \frac{3x}{2} + 1$ to $y^2 = x^3 - 3x^2 + 3x + 1$ at the point $(0, 1)$, apparently by inspection. Without mentioning its geometric interpretation, he simply substitutes $\frac{3x}{2} + 1$ for y in $y^2 = x^3 - 3x^2 + 3x + 1$.

8.3.1 Check that this substitution gives the equation

$$x^3 - \frac{21}{4}x^2 = 0.$$

What is the geometric interpretation of the double root $x = 0$?

8.3.2 What would you substitute for y to find the tangent at $(0, 1)$ to the curve $y^2 = x^3 - 3x^2 + 5x + 1$?

These examples show how tangents can be found by looking for double roots, though it requires some foresight to make the right substitution. With calculus, the process is more mechanical.

8.3.3 Derive the formula of Hudde and Sluse by differentiating $\sum a_{ij} x^i y^j = 0$ with respect to x .

8.3.4 Use differentiation to find the tangent to the folium $x^3 + y^3 = 3axy$ at the point (b, c) .

8.4 The *Arithmetica Infinitorum* of Wallis

Wallis's efforts to arithmetize geometry were noted in Section 6.6. In his *Arithmetica Infinitorum*, Wallis (1655a) made a similar attempt to arithmetize the theory of areas and volumes of curved figures. Some of his results were, understandably, equivalent to results already known. For example, he gave a proof that

$$\int_0^1 x^p dx = \frac{1}{p+1}$$

for positive integers p by showing that

$$\frac{0^p + 1^p + 2^p + \cdots + n^p}{n^p + n^p + n^p + \cdots + n^p} \rightarrow \frac{1}{p+1} \quad \text{as } n \rightarrow \infty.$$

However, he made a new approach to fractional powers, finding $\int_0^1 x^{m/n} dx$ directly rather than by consideration of the curve $y^n = x^m$, as Fermat had done. He first found $\int_0^1 x^{1/2} dx$, $\int_0^1 x^{1/3} dx$, ... by considering the areas complementary to those under $y = x^2$, $y = x^3$, ... (Figure 8.3), then guessed the results for other fractional powers by analogy with those already obtained.

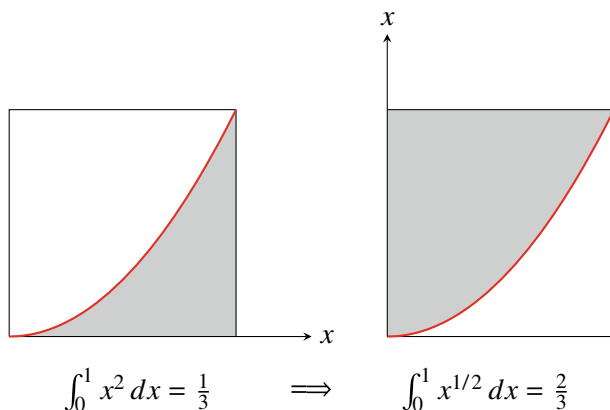


Figure 8.3: Areas used by Wallis

Like other early contributors to calculus, Wallis was ambivalent about quantities that tended to zero, treating them as nonzero one minute and zero the next. For this he received a ferocious blast from his arch-enemy

Thomas Hobbes: “Your scurvy book of *Arithmetica infinitorum*; where your indivisibles have nothing to do, but as they are supposed to have quantity, that is to say, to be *divisibles*” (Hobbes (1656), p. 301). Leaving aside this fault, which is easily remedied by limit arguments, the reasoning of Wallis is extremely incomplete by today’s standards. Observing a pattern in formulas for $p = 1, 2, 3$, for example, he will immediately claim a formula for all positive integers p “by induction” and for fractional p “by interpolation.” His boldness reached new heights toward the end of the *Arithmetica infinitorum* in deriving his famous infinite product formula,

$$\frac{\pi}{4} = \frac{2}{3} \cdot \frac{4}{3} \cdot \frac{4}{5} \cdot \frac{6}{5} \cdot \frac{6}{7} \cdots$$

An exposition of his reasoning may be found in Edwards (1979), pp. 171–176, where it is described as “one of the more audacious investigations by analogy and intuition that has ever yielded a correct result.”

However, we must bear in mind that Wallis was offering primarily a method of discovery, and what a discovery he made! His infinite product for π was not the first ever given, since Viète (1593) had discovered

$$\begin{aligned} \frac{2}{\pi} &= \cos \frac{\pi}{4} \cos \frac{\pi}{8} \cos \frac{\pi}{16} \cdots \\ &= \sqrt{\frac{1}{2}} \cdot \sqrt{\frac{1}{2} \left(1 + \sqrt{\frac{1}{2}} \right)} \cdot \sqrt{\frac{1}{2} \left[1 + \sqrt{\frac{1}{2} \left(1 + \sqrt{\frac{1}{2}} \right)} \right]} \cdots \end{aligned}$$

However, the formula of Viète is based on a clever but simple trick (see exercises), whereas that of Wallis is of deeper significance. By relating π to the integers through a sequence of rational operations, Wallis uncovered a sequence of fractions, obtained by terminating the product at the n th factor, that he called *hypergeometric*. Similar sequences were later found to occur as coefficients in series expansions of many functions, which led to a broad class of functions being called hypergeometric by Gauss. Also, Wallis’s product was closely related to two other beautiful formulas for π based on sequences of rational operations:

$$\frac{4}{\pi} = 1 + \frac{1^2}{2 + \frac{3^2}{2 + \frac{5^2}{2 + \frac{7^2}{2 + \cdots}}}}$$

and

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots.$$

The continued fraction was obtained by Brouncker from Wallis's product and also published in Wallis (1655b). The series is a special case of the series

$$\tan^{-1} x = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \cdots$$

discovered by the Indian mathematician Mādhava in the 15th century (see Section 9.2) and rediscovered by Newton, Gregory, and Leibniz. Euler (1748a), p. 311, gave a direct transformation of the series for $\pi/4$ into Brouncker's continued fraction. Besides setting off this spectacular chain reaction, Wallis's method of interpolation had important consequences in the work of Newton, who used it to discover the binomial theorem for fractional powers p (Section 9.3), where $(1+x)^p$ becomes an infinite series.

EXERCISES

8.4.1 Use the identity $\sin x = 2 \sin(x/2) \cos(x/2)$ to show that

$$\frac{\sin x}{2^n \sin(x/2^n)} = \cos \frac{x}{2} \cos \frac{x}{2^2} \cdots \cos \frac{x}{2^n},$$

whence

$$\frac{\sin x}{x} = \cos \frac{x}{2} \cos \frac{x}{2^2} \cos \frac{x}{2^3} \cdots.$$

8.4.2 Deduce Viète's product by substituting $x = \pi/2$.

The equation relating the series for $\pi/4$ to the continued fraction for $4/\pi$, namely

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \frac{1}{1 + \frac{1^2}{2 + \frac{3^2}{2 + \frac{5^2}{2 + \frac{7^2}{2 + \cdots}}}}}$$

follows immediately from a more general equation

$$\frac{1}{A} - \frac{1}{B} + \frac{1}{C} - \frac{1}{D} + \cdots = \frac{1}{A + \frac{A^2}{B - A + \frac{B^2}{C - B + \frac{C^2}{D - C + \cdots}}}}$$

proved by Euler (1748a), p. 311. The following exercises give a proof of Euler's result.

8.4.3 Check that

$$\frac{1}{A} - \frac{1}{B} = \frac{1}{A + \frac{A^2}{B - A}}.$$

8.4.4 When $\frac{1}{B}$ on the left side in Exercise 8.4.3 is replaced by $\frac{1}{B} - \frac{1}{C}$, which equals $\frac{1}{B + \frac{B^2}{C - B}}$ by Exercise 8.4.3, show that B on the right should be replaced by $B + \frac{B^2}{C - B}$. Hence show that

$$\frac{1}{A} - \frac{1}{B} + \frac{1}{C} = \frac{1}{A + \frac{A^2}{B - A + \frac{B^2}{C - B}}}.$$

Thus when we modify the tail end of the series (replacing $\frac{1}{B}$ by $\frac{1}{B} - \frac{1}{C}$), only the tail end of the continued fraction is affected. This situation continues:

8.4.5 Generalize your argument in Exercise 8.4.4 to obtain a continued fraction for a series with n terms, and hence prove Euler's equation.

8.5 Newton's Calculus of Series

Newton made many of his most important discoveries in 1665/6, after studying the works of Descartes, Viète, and Wallis. In Schooten's edition of *La Géométrie* he encountered Hudde's rule for tangents to algebraic curves, which was virtually a complete differential calculus from Newton's viewpoint. Although Newton made contributions to differentiation that are useful to *us*—the chain rule, for example—differentiation was a minor part of *his* calculus, which depended mainly on the manipulation of infinite series. Thus it is misleading to describe Newton as a founder of calculus unless one understands calculus, as he did, as an algebra of infinite series. In this calculus, differentiation and integration are carried out term by term on powers of x and hence are comparatively trivial.

At the beginning of his main work on calculus, *A Treatise of the Methods of Series and Fluxions* (also known by its abbreviated Latin name of *De methodis*), Newton likens the role of infinite series to the role of infinite decimals:

Since the operations of computing in numbers and with variables are closely similar ... I am amazed that it has occurred to no one (if you except N. Mercator with his quadrature of the hyperbola) to fit the doctrine recently established for decimal numbers in similar fashion to variables, especially since the way is then open to more striking consequences. For since this doctrine in species has the same relationship to Algebra that the doctrine in decimal numbers has to common Arithmetic, its operations of Addition, Subtraction, Multiplication, Division and Root extraction may be easily learnt from the latter's.

Newton (1671), pp. 33–35

The quadrature (area determination) of the hyperbola mentioned by Newton was the result that we would write as

$$\int_0^x \frac{dt}{1+t} = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots,$$

first published in Mercator (1668). Newton had discovered the same result in 1665, and it was partly his dismay in losing priority that led him to write *De methodis* and an earlier work *De analysi* (Newton (1669); the full title in English is *On Analysis by Equations Unlimited in Their Number of Terms*). Newton also independently discovered the series for $\tan^{-1} x$, $\sin x$, and $\cos x$ in *De analysi*, without knowing that all three series had already been discovered by Indian mathematicians. See Section 9.2.

Newton rediscovered the Mercator and Indian results by the method of expanding a geometric series and integrating term by term. In our notation,

$$\begin{aligned} \int_0^x \frac{dt}{1+t} &= \int_0^x (1 - t + t^2 - t^3 + \cdots) dt \\ &= x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots \end{aligned}$$

and

$$\begin{aligned} \tan^{-1} x &= \int_0^x \frac{dt}{1+t^2} \\ &= \int_0^x (1 - t^2 + t^4 - t^6 + \cdots) dt \\ &= x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \cdots. \end{aligned}$$

He routinely used these methods in *De analysi* and *De methodis*, but greatly extended their scope by algebraic manipulation. Not only did he find sums, products, quotients, and roots, as foreshadowed in his introduction to *De methodis*, but his root extractions also extended to the general construction of *inverse functions* by the new idea of inverting infinite series. For example, after Newton (1671), p. 61, found the series $x - (x^2/2) + (x^3/3) - \dots$, for $\int_0^x dt/(1+t)$, which is $\log(1+x)$, he set

$$y = x - \frac{x^2}{2} + \frac{x^3}{3} - \dots \quad (1)$$

and solved (1) for x (which we recognize to be the exponential function e^y , minus 1). His method amounts to setting $x = a_0 + a_1y + a_2y^2 + \dots$, substituting in the right-hand side of (1), and determining a_0, a_1, a_2, \dots in succession by comparing with the coefficients on the left-hand side. Newton found the first few terms,

$$x = y + \frac{1}{2}y^2 + \frac{1}{6}y^3 + \frac{1}{24}y^4 + \frac{1}{120}y^5 + \dots,$$

then confidently guessed that $a_n = 1/n!$ in the manner of Wallis. As he put it, "Now after the roots have been extracted to a suitable period, they may sometimes be extended at pleasure by observing the analogy of the series."

De Moivre (1698) gave a formula for inverting series that justifies such conclusions; Newton astonishes us by finding such an elegant result by such a forbidding method. His discovery of the sine series (Newton (1669), pp. 233, 237) is even more amazing. First he used the binomial series

$$(1+a)^p = 1 + pa + \frac{p(p-1)}{2!}a^2 + \frac{p(p-1)(p-2)}{3!}a^3 + \dots$$

(though not with the natural choice $a = -x^2$, $p = -\frac{1}{2}$) to obtain

$$\sin^{-1} x = z = x + \frac{1}{2} \frac{x^3}{3} + \frac{1 \cdot 3}{2 \cdot 4} \frac{x^5}{5} + \frac{1 \cdot 3 \cdot 5}{2 \cdot 4 \cdot 6} \frac{x^7}{7} + \dots$$

by term-by-term integration, and then casually stated "I extract the root, which will be

$$x = z - \frac{1}{6}z^3 + \frac{1}{120}z^5 - \frac{1}{5040}z^7 + \frac{1}{362880}z^9 - \dots"$$

adding a few lines later that the coefficient of z^{2n+1} is $1/(2n+1)!$.

EXERCISES

Newton inverted series by a tabular method like the following, which shows the coefficients of $1, y, y^2, y^3, \dots$ in x and its powers.

	1	y	y^2	y^3	\dots
x	a_0	a_1	a_2	a_3	\dots
x^2	a_0^2	$2a_0a_1$	$2a_0a_2 + a_1^2$	$2a_0a_3 + 2a_1a_2$	\dots

8.5.1 Use the rows shown to substitute series in powers of y for x and x^2 in $y = x - \frac{x^2}{2} + \dots$, and hence show that $a_0 = 0$, $a_1 = 1$, and $a_2 = 1/2$ in turn, by comparing coefficients on the two sides of the equation.

8.5.2 Compute the first few entries in the third row of the table (the coefficients of x^3), and hence show that $a_3 = 1/6$.

This shows why the inverse function $x = e^y - 1$ has a power series that begins

$$y + \frac{1}{2}y^2 + \frac{1}{6}y^3 + \dots$$

8.5.3 Show that the binomial series gives

$$\frac{1}{\sqrt{1-t^2}} = 1 + \frac{1}{2}t^2 + \frac{1 \cdot 3}{2 \cdot 4}t^4 + \frac{1 \cdot 3 \cdot 5}{2 \cdot 4 \cdot 6}t^6 + \dots$$

8.5.4 Use Exercise 8.5.3 and $\sin^{-1} x = \int_0^x dt / \sqrt{1-t^2}$ to derive Newton's series for $\sin^{-1} x$.

8.6 The Calculus of Leibniz

Newton's epoch-making works (1669, 1671) were circulated among some of his contemporaries but, incredible as it now seems, were not published at the time. The reasons seem complicated—see Westfall (1980), p. 231—but at any rate, the first published paper on calculus was not by Newton but by Leibniz (1684). This led to Leibniz's initially receiving credit for the calculus and later to a bitter dispute with Newton and his followers over the question of priority for the discovery.

There is no doubt that Leibniz discovered calculus independently, that he had a better notation, and that his followers contributed more to the spread of calculus than did Newton's. Leibniz's work lacked the depth and virtuosity of Newton's, but then Leibniz was a librarian, a philosopher, and a diplomat with only a part-time interest in mathematics. His

Nova methodus (1684) is a relatively slight paper, though it does lay down some important fundamentals—the sum, product, and quotient rules for differentiation—and it introduces the dy/dx notation we now use. However, dy/dx was not just a symbol for Leibniz, as it is for us, but literally a *quotient of infinitesimals* dy and dx , which he viewed as differences (hence the symbol d) between neighboring values of y and x , respectively.

He also introduced the integral sign, \int , in his *De geometria* (1686) and proved the fundamental theorem of calculus, that integration is the inverse of differentiation. This result was known to Newton and even, in a geometric form, to Newton’s teacher Barrow, but it became more transparent in Leibniz’s formalism. For Leibniz, \int meant “sum,” and $\int f(x) dx$ was literally a sum of terms $f(x)dx$, representing infinitesimal areas of height $f(x)$ and width dx . The difference operator d yields the last term $f(x) dx$ in the sum, and dividing by the infinitesimal dx yields $f(x)$. So voila!

$$\frac{d}{dx} \int f(x) dx = f(x)$$

—the fundamental theorem of calculus.

The Leibniz fundamental theorem can be viewed as *infinitesimal geometry* by interpreting $\int f(x) dx$ as the *area* $A(x)$ under the curve $y = f(t)$ between $t = a$ to $t = x$ (Figure 8.4). Then an infinitesimal increase in t from x to $x + dx$ increases $A(x)$ by an infinitesimal amount $dA(x)$, the area of an infinitesimal rectangle of width dx and height $f(x)$.

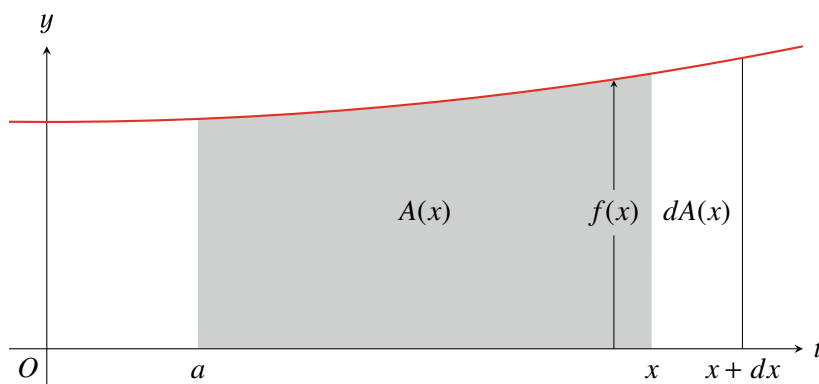


Figure 8.4: Fundamental theorem of calculus as infinitesimal geometry

Thus $A(x)$ is an *antiderivative*¹ of $f(x)$:

$$dA(x) = f(x) dx, \quad \text{and therefore} \quad \frac{dA(x)}{dx} = f(x).$$

Leibniz's strength lay in the identification of important concepts, rather than in their technical development. He introduced the word "function" and was the first to begin thinking in function terms. He made the distinction between algebraic and transcendental functions and, in contrast to Newton, preferred "closed-form" expressions to infinite series. Thus the evaluation of $\int f(x) dx$ for Leibniz was the problem of finding a known function whose derivative was $f(x)$, whereas for Newton it was the problem of expanding $f(x)$ in series, after which integration was trivial.

The search for closed forms was a wild goose chase but, like many efforts to solve intractable problems, it led to worthwhile results in other directions. Attempts to integrate rational functions raised the problem of factorization of polynomials and led ultimately to the fundamental theorem of algebra (see Chapter 11). Attempts to integrate $1/\sqrt{1-x^4}$ led to the theory of elliptic functions (Chapter 10).

As mentioned in Section 8.1, the problem of deciding which algebraic functions may be integrated in closed form has been solved only recently, though not in a way suitable for calculus textbooks, which have basically not advanced much further than Leibniz. (One thing that has changed: it is now much easier to publish a calculus book than it was for Newton!)

EXERCISES

Leibniz (1702) was stymied by the integral $\int \frac{dx}{x^4+1}$, because he did not spot the factorization of $x^4 + 1$ into real quadratic factors.

8.6.1 Writing $x^4 + 1 = x^4 + 2x^2 + 1 - 2x^2$ or otherwise, split $x^4 + 1$ into real quadratic factors.

8.6.2 Use the factors in Exercise 8.6.1 to express $\frac{1}{x^4+1}$ in the partial fraction form

$$\frac{x + \sqrt{2}}{q_1(x)} + \frac{x - \sqrt{2}}{q_2(x)},$$

where $q_1(x)$ and $q_2(x)$ are real quadratic polynomials.

8.6.3 Without working out all the details, explain how the partial fractions in Exercise 8.6.2 can be integrated in terms of rational functions and the \tan^{-1} function.

¹The fundamental theorem says that in calculus you only have to know differentiation—but you have to know it *backwards*.



9

Infinite Series

PREVIEW

As we saw in the previous chapter, many calculus problems have a solution that can be expressed as an infinite series. It is therefore useful to be able to recognize important individual series and to understand their general properties and capabilities. This is the aim of the present chapter.

Starting with the infinite geometric series, already known to Euclid, we discuss the handful of examples known before the invention of calculus. These include the *harmonic series* $1 + 1/2 + 1/3 + 1/4 + \dots$, studied by Oresme around 1350, and the stunning series for the inverse tangent, sine, and cosine, discovered by Indian mathematicians in the 15th century.

The invention of calculus in the 17th century released a flood of new series, mostly of the form $a_0 + a_1x + a_2x^2 + \dots$ (called *power series*), but also some variations, such as generalizations of the harmonic series.

Euler (1748a) introduced the generalization

$$1 + 1/2^s + 1/3^s + 1/4^s + \dots,$$

whose value for $s = 2$, he had already shown to be $\pi^2/6$. He also showed that, for $s > 1$, the series equals the *infinite product*

$$(1 - 1/2^s)^{-1}(1 - 1/3^s)^{-1}(1 - 1/5^s)^{-1} \dots (1 - 1/p^s)^{-1} \dots$$

over all the *prime* numbers p . This discovery of Euler's opened a new path to the secrets of the primes, exploration of which continues to this day.

The book Euler (1748a), whose full title is *Introduction to the Analysis of the Infinite*, was intended by Euler to be preparation for calculus. Infinite sums and products were the “pre-calculus” of the 18th century!

9.1 Early Results

Infinite series were present in Greek mathematics, though the Greeks tried to deal with them as finitely as possible by working with arbitrary finite sums $a_1 + a_2 + \cdots + a_n$ instead of infinite sums $a_1 + a_2 + \cdots$. However, this is just the difference between potential and actual infinity. There is no question that Zeno's paradox of the dichotomy (Section 4.1), for example, concerns the decomposition of the number 1 into the infinite series

$$\frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^4} + \cdots$$

and that Archimedes found the area of the parabolic segment (Section 4.4) essentially by summing the infinite series

$$1 + \frac{1}{4} + \frac{1}{4^2} + \frac{1}{4^3} + \cdots = \frac{4}{3}.$$

Both these examples are special cases of the result we express as summation of a geometric series

$$a + ar + ar^2 + ar^3 + \cdots = \frac{a}{1-r} \quad \text{when } |r| < 1.$$

The first examples of infinite series other than geometric series appeared in the Middle Ages. In a book from around 1350, called the *Liber calculationum*, Richard Suiseth (or Swineshead, known as the Calculator) used a very lengthy verbal argument to show that

$$\frac{1}{2} + \frac{2}{2^2} + \frac{3}{2^3} + \frac{4}{2^4} + \cdots = 2.$$

The argument is reproduced in Boyer (1959), p. 78. At about the same time, Oresme (1350b), pp. 413–421, summed this and similar series by geometric decomposition as in Figure 9.1, showing that

$$2 = \frac{1}{2} + \frac{2}{2^2} + \frac{3}{2^3} + \frac{4}{2^4} + \cdots.$$

Actually Oresme gives only the last picture in the figure, but it seems likely he arrived at it by cutting up an area of two square units as shown, judging from his opening remark: “A finite surface can be made as long as we wish, or as high, by varying the extension without increasing the size.” The region constructed by Oresme, incidentally, is perhaps the first

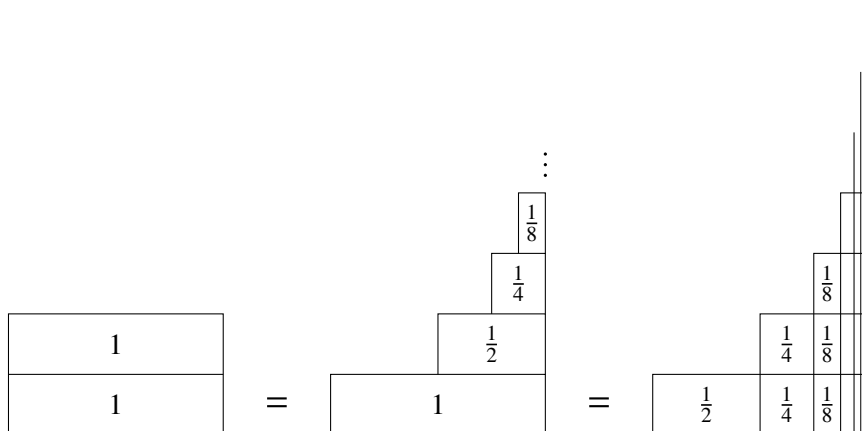


Figure 9.1: Oresme's summation

example of the phenomenon encountered by Torricelli (Section 8.2) in his hyperbolic solid of revolution—infinite extent but finite content.

Another important discovery of Oresme (1350a) was the divergence of the *harmonic series*

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \cdots .$$

His proof was by an elementary argument that is now standard:

$$\begin{aligned} & 1 + \left(\frac{1}{2}\right) + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \cdots \\ & > 1 + \left(\frac{1}{2}\right) + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + \cdots \\ & = 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \cdots . \end{aligned}$$

Thus by repeatedly doubling the number of terms collected in successive groups, we can indefinitely obtain groups of sum $> \frac{1}{2}$, enabling the sum to grow beyond all bounds.

EXERCISES

Oresme's proof by partitioning the harmonic series into

$$1 + \left(\frac{1}{2}\right) + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \cdots$$

has the following geometric counterpart.

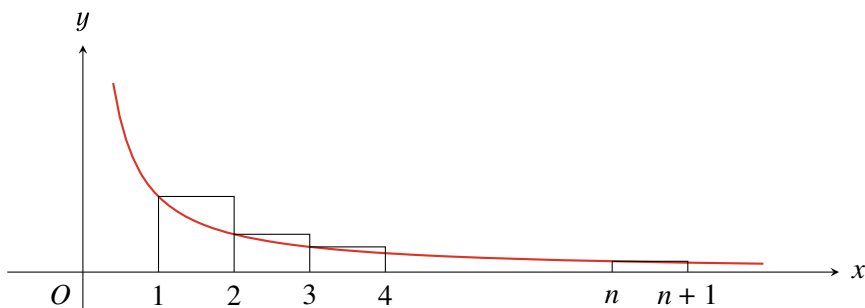


Figure 9.2: Comparing $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ with an area

9.1.1 By referring to Figure 9.2, show that

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} > \text{area under } y = \frac{1}{x} \text{ between } x = 1 \text{ and } x = n + 1.$$

9.1.2 Now partition this area under $y = 1/x$ into the pieces between $x = 1$ and $x = 2$, $x = 2$ and $x = 4$, $x = 4$ and $x = 8$, \dots , and show that *all these pieces have the same area*. (This can even be done without using calculus, if you use the argument of Exercises 4.4.1 and 4.4.2.)

9.1.3 Deduce from Exercise 9.1.2 that the area from $x = 1$ to $x = n$, and hence the sum $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$, tends to infinity.

The area under $y = 1/x$ from $x = 1$ to $x = n + 1$ is of course $\log(n + 1)$, so Figure 9.2 shows that $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} > \log(n + 1)$. As $n \rightarrow \infty$, these two functions of n remain about the same size.

9.1.4 By comparing the curved area with suitable rectangles beneath the curve, show that

$$\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} < \log(n + 1),$$

and hence that $0 < 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log(n + 1) < 1$.

9.1.5 Also show, by a geometric argument, that $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log(n + 1)$ increases as n increases, so that it has a finite limit < 1 .

The value of the limit is known as *Euler's constant* γ , and γ is approximately 0.577. However, little is known about the nature of γ —not even whether it is irrational.

9.2 From Pythagoras to Pi

As mentioned in Section 8.4, the Indian mathematician Mādhava found the series

$$\tan^{-1} x = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \cdots$$

with its important special case

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots$$

in the 15th century. The series for π was the first satisfactory answer to the classical problem of squaring the circle, for although the expression is infinite (as it must be, by Lindemann's theorem on the transcendence of π), the rule producing successive terms is as finite and transparent as could be. Sadly, the Indian series became known in the West too late to have any influence or even to become well known until recently. Rajagopal and Rangachari (1977, 1986) showed that the series for $\tan^{-1} x$, $\sin x$, and $\cos x$ were known in the Kerala school of Mādhava before 1540, and probably before 1500. For more recent information on the Kerala school, in the context of trigonometry and of Indian mathematics in general, see Van Brummelen (2009) and Plofker (2009) respectively.

In this section we give a streamlined derivation of the Mādhava series for π , bypassing the trigonometry and using only a little calculus. Our starting point is the pair of equations found in Section 1.3:

$$x = \frac{1 - t^2}{1 + t^2}, \quad y = \frac{2t}{1 + t^2}.$$

There, we used these equations only for rational values of t , in order to find all rational points (x, y) on the unit circle and hence all Pythagorean triples. Here, we use them for all *real* values of t to describe the whole circle, except for the point $(-1, 0)$, by two *rational functions* of t . The beauty of this description is that it is amenable to basic calculus—in particular, differentiation of rational functions.

For any curve given parametrically by $x = f(t)$, $y = g(t)$ the distance Δs between points with parameter values t and $t + \Delta t$ is

$$\Delta s = \sqrt{\left(\frac{\Delta x}{\Delta t}\right)^2 + \left(\frac{\Delta y}{\Delta t}\right)^2} \Delta t,$$

where $\Delta x = f(t + \Delta t) - f(t)$, $\Delta y = g(t + \Delta t) - g(t)$. This is because of the Pythagorean theorem, which says that the distance Δs between the points (x, y) and $(x + \Delta x, y + \Delta y)$ is given (see Figure 9.3) by

$$(\Delta s)^2 = (\Delta x)^2 + (\Delta y)^2.$$

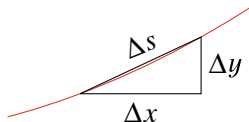


Figure 9.3: Approaching arc length via the Pythagorean theorem

It follows, by letting $\Delta t \rightarrow 0$, that the arc length of the circle between parameter values $t = a$ and $t = b$ is the integral

$$\int_a^b \sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2} dt. \quad (*)$$

Now, differentiating the equations $x = \frac{1-t^2}{1+t^2}$, $y = \frac{2t}{1+t^2}$ gives

$$\frac{dx}{dt} = -\frac{4t}{(1+t^2)^2} = -\frac{2y}{1+t^2} \quad \text{and} \quad \frac{dy}{dt} = \frac{2-2t^2}{(1+t^2)^2} = \frac{2x}{1+t^2}.$$

When these expressions are substituted in the arc length integral (*) we get, thanks to the fact that $x^2 + y^2 = 1$,

$$\int_a^b \frac{2 dt}{1+t^2}.$$

It is also clear, since t is the slope of the line through $(-1, 0)$ in Section 1.3, that we get one quarter of the circle as t runs from 0 to 1. So, defining π to be the length of the semicircle, we have

$$\frac{\pi}{2} = \int_0^1 \frac{2 dt}{1+t^2}, \quad \text{or, equivalently,} \quad \frac{\pi}{4} = \int_0^1 \frac{dt}{1+t^2}.$$

The latter is the integral usually found by trigonometric considerations, such as $\tan^{-1} 1 = \pi/4$. We now conclude in the usual way, expanding $\frac{1}{1+t^2}$

as the geometric series $1 - t^2 + t^4 - t^6 + \dots$:

$$\begin{aligned}\frac{\pi}{4} &= \int_0^1 \frac{dt}{1+t^2} = \int_0^1 (1 - t^2 + t^4 - t^6 + \dots) dt \\ &= \left[t - \frac{t^3}{3} + \frac{t^5}{5} - \frac{t^7}{7} + \dots \right]_0^1 \\ &= 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots.\end{aligned}$$

EXERCISES

The proof above skates over one delicate point: the infinite geometric series expansion

$$\frac{1}{1+t^2} = 1 - t^2 + t^4 - t^6 + \dots.$$

This expansion is valid only for $|t| < 1$, whereas we allowed $t = 1$ in the integration. This problem can be fixed by considering *finite* geometric series, which can be integrated without fear.

9.2.1 Show that $1 + a + a^2 + \dots + a^n = \frac{1-a^{n+1}}{1-a}$ for $a \neq 1$ and hence that

$$\frac{1}{1-a} = 1 + a + a^2 + \dots + a^n + \frac{a^{n+1}}{1-a} \quad \text{for } a \neq 1.$$

9.2.2 Conclude from Exercise 9.2.1 that

$$\frac{1}{1+t^2} = 1 - t^2 + t^4 - \dots + (-1)^n t^{2n} + (-1)^{n+1} \frac{t^{2n+2}}{1+t^2} \quad \text{for all } t.$$

9.2.3 Replacing $\frac{1}{1+t^2}$ in the integral by $1 - t^2 + t^4 - \dots + (-1)^n t^{2n} + (-1)^{n+1} \frac{t^{2n+2}}{1+t^2}$, show that

$$\frac{\pi}{4} - \left[1 - \frac{1}{3} + \frac{1}{5} - \dots + (-1)^n \frac{1}{2n+1} \right] = \pm \int_0^1 \frac{t^{2n+2}}{1+t^2} dt.$$

9.2.4 Explain why $\int_0^1 \frac{t^{2n+2}}{1+t^2} dt \leq \int_0^1 t^{2n+2} dt = \frac{1}{2n+3}$, and hence that

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots.$$

9.3 Power Series

The Indian series for $\tan^{-1} x$ was the first example, apart from geometric series such as $1 + x + x^2 + x^3 + \cdots = 1/(1 - x)$, of a *power series*, that is, the expansion of a function $f(x)$ in powers of x . The idea of power series turned out to be fruitful not only in the representation of functions but even in the study of numerical series. Most of the interesting numerical series turned out to be instances of power series for particular values of x , for example, the series for $\pi/4$ is the $x = 1$ instance of the series for $\tan^{-1} x$.

The theory began with the series published by Mercator (1668):

$$\log(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots.$$

As we have seen, this was obtained by integrating the geometric series

$$\frac{1}{1 + x} = 1 - x + x^2 - x^3 + \cdots$$

term by term. Now the most important transcendental functions—logs, exponentials, and the related circular and hyperbolic functions—are obtained by integration and inversion from algebraic functions, and fairly simple algebraic functions at that. For example, e^y is the inverse function of $y = \log x$, and

$$\log(1 + x) = \int_0^x \frac{dt}{1 + t},$$

$\sin y$ is the inverse function of $y = \sin^{-1} x$ and

$$\sin^{-1} x = \int_0^x \frac{dt}{\sqrt{1 - t^2}}, \quad \tan^{-1} x = \int_0^x \frac{dt}{1 + t^2},$$

and so on. Thus the key to finding power series is finding series expansions of simple algebraic functions. Once this is done, term-by-term integration and Newton's method of series inversion (Section 8.5) yield power series for most of the common functions.

Rational functions, such as $1/(1 + t^2)$, can be expanded using geometric series. Newton (1665a) made a crucial advance when he discovered the general binomial theorem,

$$(1 + x)^p = 1 + px + \frac{p(p-1)}{2!}x^2 + \frac{p(p-1)(p-2)}{3!}x^3 + \cdots,$$

yielding the expansion of functions such as $1/\sqrt{1-t^2} = (1-t^2)^{-1/2}$. This theorem was also discovered independently by Gregory (1670). Both Newton and Gregory were inspired by the loose heuristic method of interpolation used by Wallis (1655a), but they refined it into a result now known as the *Gregory–Newton interpolation formula*:

$$f(a+h) = f(a) + \frac{h}{b}\Delta f(a) + \frac{(h/b)(h/b-1)}{2!}\Delta^2 f(a) + \cdots, \quad (1)$$

where

$$\Delta f(a) = f(a+b) - f(a),$$

$$\Delta^2 f(a) = \Delta f(a+b) - \Delta f(a) = f(a+2b) - 2f(a+b) + f(a),$$

$$\Delta^3 f(a) = \Delta^2 f(a+b) - \Delta^2 f(a) = f(a+3b) - 3f(a+2b) + 3f(a+b) - f(a),$$

$$\vdots$$

This wonderful formula finds the value of f at an arbitrary point $a+h$ from the values at an infinite arithmetic sequence of points $a, a+b, a+2b, \dots$.

The first n terms give an n th-degree polynomial in h taking the same values as f at $a, a+b, \dots, a+nb$. Hence the formula is valid for any f that is the limit of its own approximating polynomials. This means all functions representable by power series, provided that the points $a, a+b, a+2b, \dots$, are sensibly chosen. (The points $\pi, 2\pi, 3\pi, \dots$, are a bad choice for $\sin x$, since the x -axis is a polynomial curve through all of them).

Newton discovered the formula (1) after his special investigations on interpolation that led to the binomial theorem. Independently of Newton, Gregory discovered the general formula first and derived the binomial theorem from it (see exercises below). It even appears that Gregory used the interpolation theorem to discover Taylor's theorem 44 years before Brook Taylor. The Taylor series

$$f(a+h) = f(a) + hf'(a) + \frac{h^2}{2!}f''(a) + \cdots \quad (2)$$

is just the limiting case of (1) as $b \rightarrow 0$. Indeed, this is how it was derived by Taylor (1715). The passage from (1) and (2) is simple if one assumes plausible limiting behavior for the infinite sum. Notice that

$$\frac{\Delta f(a)}{b} = \frac{f(a+b) - f(a)}{b} \rightarrow f'(a) \quad \text{as } b \rightarrow 0$$

and similarly

$$\frac{\Delta^2 f(a)}{b^2} \rightarrow f''(a), \quad \frac{\Delta^3 f(a)}{b^3} \rightarrow f'''(a),$$

and so on. We write (1) as

$$f(a+h) = f(a) + h \frac{\Delta f(a)}{b} + \frac{h(h-b)}{2!} \frac{\Delta^2 f(a)}{b^2} + \cdots$$

and observe that the n th term

$$\frac{h(h-b)(h-2b) \cdots (h-(n-1)b)}{n!} \frac{\Delta^n f(a)}{b^n} \rightarrow \frac{h^n}{n!} f^{(n)}(a) \quad \text{as } b \rightarrow 0.$$

Assuming that the limit of the infinite sum is the sum of these limits, we then get Taylor's series (2) as the limit of (1) as $b \rightarrow 0$.

An Interpolation on Interpolation

The importance of interpolation in the development of calculus seems to have been greatly underestimated. The topic rarely appears in calculus books today, and then only as a numerical method. Yet three of the most important founders of calculus, Newton, Gregory, and Leibniz, began their work with interpolation, and we have seen how this led to two of their most important results, the binomial theorem and Taylor's theorem. (For Leibniz's work, see Hofmann (1974).) When interpolation is relegated to numerical methods, this connection is lost. Of course, interpolation *is* a numerical method in practice, when one uses only a few terms of the Gregory–Newton series, but the full series is exact and hence much more interesting. It was interest in infinite expansions per se that distinguished Newton, Gregory, and Leibniz (as well as Wallis) from their predecessors in interpolation.

Interpolation goes back to ancient times as a method for estimating the values of functions between known values. But perhaps the first to glimpse the possibility of exact interpolation were Thomas Harriot (1560–1621) and Henry Briggs (1556–1630). A formula has been found in Harriot's papers that is equivalent to the first terms of the Gregory–Newton series; see Lohne (1965). Lohne dates this work of Harriot at 1611. Briggs may have learned something about interpolation from Harriot when the two were at Oxford around 1620. Briggs's *Arithmetica logarithmica* (1624), which is concerned with the calculation of logarithms, uses series for

interpolation, and in the process gives the first instance of the binomial theorem for a fractional exponent

$$(1+x)^{1/2} = 1 + \frac{1}{2}x - \frac{1 \cdot 1}{2 \cdot 4}x^2 + \frac{1 \cdot 1 \cdot 3}{2 \cdot 4 \cdot 6}x^3 - \frac{1 \cdot 1 \cdot 3 \cdot 5}{2 \cdot 4 \cdot 6 \cdot 8}x^4 + \cdots.$$

Gregory knew of Briggs's work, and Newton certainly *could* have known of it, though no strong evidence that he did has yet been found. For more information on the history of interpolation, see Whiteside (1961) and Goldstine (1977).

EXERCISES

Here is how to derive the general binomial series from the Gregory–Newton interpolation formula.

9.3.1 Show that

$$\Delta^n f(a) = \sum_{i=0}^n (-1)^{n-i} \binom{n}{i} f(a + ib),$$

where $\binom{n}{i}$ is the ordinary binomial coefficient.

9.3.2 If $a = 0$, $b = 1$, and $f(x) = (1+k)^x$, show that $\Delta^n f(0) = k^n$ using the finite binomial series

$$(1+h)^n = \sum_{i=0}^n \binom{n}{i} h^i.$$

9.3.3 Deduce the general binomial series

$$(1+k)^x = 1 + xk + \frac{x(x-1)}{2!}k^2 + \frac{x(x-1)(x-2)}{3!}k^3 + \cdots$$

using the Gregory–Newton interpolation formula.

9.4 Fractional Power Series

Power series helped to make mathematicians aware of the function concept by revealing the generality of the expression $a_0 + a_1x + a_2x^2 + \cdots$. However, not every function $f(x)$ is expressible as $a_0 + a_1x + a_2x^2 + \cdots$. This is obvious for functions that tend to infinity as $x \rightarrow 0$, since the power series has value a_0 when $x = 0$. For other functions, such as $f(x) = x^{1/2}$, the behavior at 0 disallows a power-series expansion for a more subtle reason. These functions have *branching behavior* at 0; they are *many-valued*, and hence they are not functions in the strict sense. The function $x^{1/2}$, for

example, is two-valued because each number has two square roots, one the negative of the other.

Such behavior does not occur for a power series $a_0 + a_1x + a_2x^2 + \cdots$, which has only one value for each value of x . All fractional powers of x are many-valued— $x^{1/3}$ is three-valued, $x^{1/4}$ is four-valued, and so on. Many-valued behavior is typical of algebraic functions, where y is said to be an *algebraic function of x* if x and y satisfy a polynomial equation $p(x, y) = 0$. Since most polynomial equations are not solvable by radicals (Section 5.7), most algebraic functions are not given by finite expressions built from $+$, $-$, \times , \div , and fractional powers.

However, it was the remarkable discovery of Newton (1671) that any algebraic function y can be expressed as a *fractional power series* in x :

$$y = a_0 + a_1x^{r_1} + a_2x^{r_2} + a_3x^{r_3} + \cdots,$$

where r_1, r_2, r_3, \dots , are rational numbers. Furthermore, the series can be rewritten in the form

$$\begin{aligned} & a_0 + b_1x^{s_1}(c_{00} + c_{01}x + c_{02}x^2 + \cdots) \\ & + b_2x^{s_2}(c_{10} + c_{11}x + c_{12}x^2 + \cdots) \\ & \vdots \\ & + b_nx^{s_n}(c_{n0} + c_{n1}x + c_{n2}x^2 + \cdots) \end{aligned}$$

that is, as a finite sum of ordinary power series with fractional powers of x as multipliers. Near $x = 0$, y behaves like a finite sum of fractional powers.

For example, if $y^2(1+x)^2 = x$, we have

$$\begin{aligned} y &= \frac{x^{1/2}}{1+x} \\ &= x^{1/2}(1 - x + x^2 - x^3 + \cdots), \end{aligned}$$

and near the origin, y has behavior similar to $x^{1/2}$; in particular there are two values of y for each x . Newton's contribution was an ingenious algorithm for obtaining the successive powers of x . The fractional powers themselves were not properly understood until the variables x and y were taken to be complex. This was done in the 19th century, and on this basis a more rigorous derivation of Newton's series was given by Puiseux (1850). For this reason, the fractional power-series expansions of algebraic functions are now called *Puiseux expansions*.

EXERCISE

The impossibility of an ordinary power series for $x^{1/2}$ can be shown as follows.

9.4.1 Any ordinary power-series expansion of $x^{1/2}$ would have to be of the form

$$x^{1/2} = a_1x + a_2x^2 + a_3x^3 + \cdots$$

because $x^{1/2} = 0$ when $x = 0$. Now square both sides and deduce a contradiction.

9.5 Summation of Series

The results on infinite series seen so far are mostly decompositions or expansions rather than summations. That is, a known quantity or function is decomposed into an infinite series. Solutions of the converse problem, finding the sum of a given series, were comparatively rare. Archimedes' summation of $1 + 1/4 + 1/4^2 + \cdots$ was one. Perhaps the next were of series such as $1/1 \cdot 2 + 1/2 \cdot 3 + \cdots + 1/n(n+1) + \cdots$, given by Mengoli (1650). The series $\sum 1/n(n+1)$ is easily summed because of the happy accident that

$$\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1},$$

whence

$$\begin{aligned} \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n(n+1)} &= \left(1 - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \cdots + \left(\frac{1}{n} - \frac{1}{n+1}\right) \\ &= 1 - \frac{1}{n+1}. \end{aligned}$$

By letting $n \rightarrow \infty$ we then obtain the sum 1 for the infinite series.

The first really tough summation problem was $1 + 1/2^2 + 1/3^2 + \cdots$. Mengoli tackled this without success, as did the brothers Jakob and Johann Bernoulli in a series of papers (1704). The Bernoulli brothers were able to sum similar series, rediscovering Mengoli's $\sum 1/n(n+1)$ and also summing $\sum 1/(n^2-1)$, but for $\sum 1/n^2$ itself they could obtain only trivial results such as

$$\frac{1}{2^2} + \frac{1}{4^2} + \frac{1}{6^2} + \cdots = \frac{1}{4} \left(1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots\right).$$

The solution was finally obtained by Euler (1734), long after the death of Jakob Bernoulli, and Johann Bernoulli exclaimed, "In this way my

brother's most ardent wish is satisfied ...if only my brother were still alive!" (Johann Bernoulli, *Opera*, Vol. 4, p. 22). In fact, after hearing that the sum is $\pi^2/6$, Johann Bernoulli himself discovered a proof, which turned out to be the same as Euler's.

Euler (1707–1783) was the greatest virtuoso of series manipulation, and his first summation of $1 + 1/2^2 + 1/3^2 + \cdots$ was one of his most audacious. (Later he gave more rigorous proofs.) Consider the equation

$$\frac{\sin \sqrt{x}}{\sqrt{x}} = 1 - \frac{x}{3!} + \frac{x^2}{5!} - \frac{x^3}{7!} + \cdots = 0, \quad (1)$$

easily obtained from the sine series of Section 8.5. This equation has roots $x_1 = \pi^2$, $x_2 = (2\pi)^2$, $x_3 = (3\pi)^2$, ..., but *not* 0, because $\sin \sqrt{x}/\sqrt{x} \rightarrow 1$ as $x \rightarrow 0$. Now if a *polynomial* equation

$$1 + a_1x + a_2x^2 + \cdots + a_nx^n = 0$$

has roots $x = x_1, x_2, \dots, x_n$, Descartes's factor theorem (Section 5.7) gives

$$1 + a_1x + \cdots + a_nx^n = \left(1 - \frac{x}{x_1}\right)\left(1 - \frac{x}{x_2}\right)\cdots\left(1 - \frac{x}{x_n}\right). \quad (2)$$

Also

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n} = -\text{coefficient of } x = -a_1,$$

since each x term in the expansion of the right-hand side of (2) comes from a term $-x/x_i$ in one factor multiplied by 1's in all the other factors. Assuming that this is also true of the "infinite polynomial" equation (1), we get

$$\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} + \cdots = -\text{coefficient of } x = -\left(-\frac{1}{3!}\right),$$

that is,

$$\frac{1}{\pi^2} + \frac{1}{(2\pi)^2} + \frac{1}{(3\pi)^2} + \cdots = \frac{1}{6}.$$

Hence

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}. \quad (\text{Q.E.D.!!})$$

The extraordinary and beautiful world of formulas revealed by Euler is today somewhat neglected in mathematics instruction. For a history of mathematics with an emphasis on infinite formulas, see Roy (2011).

EXERCISES

Euler's reasoning also leads to a correct infinite product formula for $\sin x$, which in turn gives the Wallis product for $\pi/4$ (Section 8.4).

9.5.1 Deduce an infinite product for $\frac{\sin \sqrt{x}}{\sqrt{x}}$ from Euler's reasoning, and hence show that

$$\sin x = x \left(1 - \frac{x^2}{\pi^2}\right) \left(1 - \frac{x^2}{2^2\pi^2}\right) \left(1 - \frac{x^2}{3^2\pi^2}\right) \cdots.$$

9.5.2 By substituting $x = \pi/2$ in the infinite product for $\sin x$, show that

$$\frac{2}{\pi} = \frac{1 \cdot 3}{2 \cdot 2} \cdot \frac{3 \cdot 5}{4 \cdot 4} \cdot \frac{5 \cdot 7}{6 \cdot 6} \cdots,$$

and hence obtain Wallis's product for $\pi/4$.

9.6 The Zeta Function

The sum $1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots$ first drew Euler's attention to the function now known as the *zeta function*:

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$$

This function is well-defined for real values of $s > 1$, and Euler's initial discovery was that $\zeta(2) = \pi^2/6$. Later, he also found the values of $\zeta(s)$ for $s = 4, 6, 8, \dots$. But his most spectacular discovery was the *product formula* of Euler (1748a), p. 288, showing that $\zeta(s)$ encodes the sequence 2, 3, 5, 7, 11, ..., of *prime numbers*. Euler's formula is

$$\begin{aligned} & \frac{1}{(1 - 1/2^s)} \frac{1}{(1 - 1/3^s)} \frac{1}{(1 - 1/5^s)} \frac{1}{(1 - 1/7^s)} \frac{1}{(1 - 1/11^s)} \cdots \\ &= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots. \end{aligned}$$

The factors on the left-hand side are $(1 - 1/p_n^s)^{-1}$, where p_n is the n th prime. To see why these factors give the terms on the right-hand side we expand each of them as a geometric series

$$1 + \frac{1}{p_n^s} + \frac{1}{p_n^{2s}} + \frac{1}{p_n^{3s}} + \cdots.$$

Multiplying all these series together, we get the reciprocal of each possible product of primes, to the s th power, exactly once. That is, the left-hand side is the sum

$$1 + \sum \frac{1}{p_1^{m_1 s} p_2^{m_2 s} \cdots p_r^{m_r s}} = 1 + \sum \frac{1}{(p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r})^s},$$

in which each product $p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ of primes occurs exactly once. But each natural number ≥ 2 is expressible in just one way as a product of primes (Section 3.3), hence the latter sum equals the right-hand side of Euler's formula

$$1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots.$$

Initially the exponent $s > 1$ was there only to ensure convergence. We saw in Section 9.1 that $\zeta(s)$ diverges when $s = 1$; it converges when $s > 1$. Riemann (1859) discovered that $\zeta(s)$ becomes much more powerful when s is taken to be a complex variable. In recognition of this, $\zeta(s)$ is often called the *Riemann zeta function*. As mentioned above, the result of Section 9.5 shows $\zeta(2) = \pi^2/6$. The values of $\zeta(4)$, $\zeta(6)$, $\zeta(8)$, \dots , also found by Euler, turn out to be rational multiples of π^4 , π^6 , π^8 , \dots , respectively. The values of $\zeta(3)$, $\zeta(5)$, \dots have no known relationship to π or other standard constants, though Apéry (1981) showed that $\zeta(3)$ is irrational. The most famous conjecture about $\zeta(s)$, and one of the most sought-after results in mathematics today, is known as the *Riemann hypothesis*: $\zeta(s) = 0$ only when s has real part $\frac{1}{2}$ (excluding the *trivial zeros* described below).

EXERCISES

Although $\zeta(s)$ is not defined for $s = 1$ (because this gives the divergent series $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$), this situation can be exploited to give a new proof that there are infinitely many primes. (Thus the Euler product formula encapsulates two apparently unrelated results—unique prime factorization, and the infinite number of primes.)

9.6.1 (Euler) Show that if there are only finitely many primes p_1, \dots, p_n , then

$$\frac{1}{1 - 1/p_1} \cdot \frac{1}{1 - 1/p_2} \cdots \frac{1}{1 - 1/p_n} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots.$$

Deduce that there are infinitely many primes.

The statement of the Riemann hypothesis needs some qualification, because $\zeta(s)$ can be defined for certain values of s for which the series $1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$

is not meaningful. This follows from the formula

$$\zeta(1-s) = 2(2\pi)^{-s} \cos \frac{s\pi}{2} \Gamma(s) \zeta(s)$$

discovered by Riemann and called the *functional equation* for the zeta function. The functional equation enables us to define $\zeta(1-s)$ when $\zeta(s)$ is known, and it also shows that there are certain trivial zeros of $\zeta(1-s)$, namely, where s satisfies $\cos \frac{s\pi}{2} = 0$.

9.6.2 Which s give a trivial zero of $\zeta(1-s)$?

The function Γ in the functional equation is the *gamma function*, introduced by Euler to extend the factorial function, $\Gamma(n) = (n-1)!$, to non-integer values of n . An amusing consequence of the functional equation is that we can assign values to certain divergent series, such as $1 + 2 + 3 + 4 + \cdots$, by interpreting them as $\zeta(1-s)$, then reinterpreting $\zeta(1-s)$ by the functional equation.

9.6.3 By suitable reinterpretation, show that

$$1 + 2 + 3 + 4 + \cdots = -1/12.$$

Euler (1770a), p. 157, found another trick for the zeta function: giving a natural formula for the seemingly *unnatural* Euler constant γ . Recall from Exercise 9.1.5 that γ is defined to be the limit of $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log(n+1)$ as $n \rightarrow \infty$.

9.6.4 Using the Mercator series for $\log(1 + \frac{1}{k})$, show that

$$\frac{1}{k} - \log(k+1) + \log(k) = \frac{1}{2k^2} - \frac{1}{3k^3} + \frac{1}{4k^4} - \cdots.$$

9.6.5 By adding the instances of the formula in Exercise 9.6.4 from $k = 1$ to $k = n$, show that

$$\begin{aligned} & \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right) - \log(n+1) = \\ & \frac{1}{2} \left(\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{n^2}\right) - \frac{1}{3} \left(\frac{1}{1^3} + \frac{1}{2^3} + \cdots + \frac{1}{n^3}\right) + \frac{1}{4} \left(\frac{1}{1^4} + \frac{1}{2^4} + \cdots + \frac{1}{n^4}\right) - \cdots. \end{aligned}$$

9.6.6 Deduce from Exercise 9.6.5 that $\gamma = \frac{\zeta(2)}{2} - \frac{\zeta(3)}{3} + \frac{\zeta(4)}{4} - \frac{\zeta(5)}{5} + \cdots$.



10

Elliptic Curves and Functions

PREVIEW

Number theory revived in Europe with the rediscovery of Diophantus by Bombelli, and the publication of a new edition by Bachet de Méziriac (1621). It was this book that inspired Fermat and launched number theory as a modern mathematical discipline—one that draws on resources from all parts of mathematics.

Fermat mastered and extended the techniques of Diophantus, such as the chord and tangent method for finding rational points on cubic curves. This was the beginning of the modern theory of *elliptic curves*, which take their name, in a roundabout way, from what are called *elliptic functions*.

Elliptic functions, like many innovations in mathematics, arose as a way around an impasse: that no “known” function $f(x)$ has derivative $1/\sqrt{1-x^4}$. Eventually, mathematicians accepted the fact that $\int_0^x \frac{dt}{\sqrt{1-t^4}}$ is a *new* function. It is one of a family called the *elliptic integrals*, because one of them is the integral that defines the arc length of the ellipse.

Around 1800 Gauss realized that, rather than studying $u = \int_0^x \frac{dt}{\sqrt{1-t^4}}$, one should study its *inverse* function x as a function of u (just as one should study the sine function rather than the arcsine integral $\int_0^x \frac{dt}{\sqrt{1-t^2}}$). Gauss wrote $x = sl(u)$ and found that the function sl , like the sine, is *periodic*; that is, $sl(u + 2\varpi) = sl(u)$, where ϖ is a certain real number.

More surprisingly, sl has second period $2i\varpi$, so sl is better viewed as a function of *complex* numbers. These results first became widely known when they were rediscovered, published, and extended by Abel and Jacobi in the 1820s.

10.1 Fermat's Last Theorem

On the other hand, it is impossible for a cube to be written as a sum of two cubes or a fourth power to be written as a sum of two fourth powers or, in general, for any number which is a power higher than second to be written as a sum of two like powers. I have a truly marvellous demonstration of this proposition which this margin is too small to contain.

Fermat (1670), p. 241

This remark, written in the margin of his copy of Bachet's *Diophantus* when he was studying that work in the late 1630s, is the second item in Fermat's *Observations on Diophantus*, published posthumously in 1670. Fermat was responding to Diophantus's treatment of the problem of expressing a square as a sum of two squares. As we saw in Chapter 1, this is the problem of finding Pythagorean triples (a, b, c) or, equivalently, of finding the rational points $(a/c, b/c)$ on the circle $x^2 + y^2 = 1$.

Fermat's last theorem, the claim that there are no triples (a, b, c) of positive integers such that

$$a^n + b^n = c^n, \quad \text{where } n > 2 \text{ is an integer,}$$

became the most famous problem in mathematics. It was finally proved by Wiles (1995) and then only with a deep and unexpected intervention by the theory of *elliptic curves*, which we introduce below in Section 10.5. As far as we know, Fermat himself proved it only for $n = 4$. However, his proof was interesting and fruitful enough to be worth describing here—not least because it too touches on elliptic curves. It began with a problem about right-angled triangles.

Rational Right-Angled Triangles

The area of a right-angled triangle the sides of which are rational numbers cannot be a square number. This proposition, which is my own discovery, I have at length succeeded in proving, though not without much labour and hard thinking. I give the proof here, as this method will enable extraordinary developments to be made in the theory of numbers.

Fermat (1670), p. 271

This is number 45 of Fermat's *Observations on Diophantus*, responding to a problem posed by Bachet: to find a right-angled triangle whose area equals a given number. The observation is important not only for the theorem and the method announced, but also because it is followed by the only reasonably complete proof left by Fermat in number theory. As a bonus, the proof implicitly settles Fermat's last theorem for $n = 4$ (see exercises) and is an excellent illustration of his method of *infinite descent*, which did indeed lead to extraordinary developments in the theory of numbers. In what follows, the statements that make up Fermat's proof, appearing indented like the quote above, are expanded and expressed in modern notation following the reconstruction of Zeuthen (1903), p. 163. We use the translation of Fermat given by Heath (1910), p. 293, in his version of the reconstruction.

If the area of a right-angled triangle were a square, there would exist two biquadrates the difference of which would be a square number. Consequently there would exist two square numbers the sum and difference of which would be squares.

By choosing a suitable unit of length, we can express the sides of a rational right triangle as a Pythagorean triple of relatively prime integers $p^2 - q^2$, $2pq$, $p^2 + q^2$, as noted in Section 1.2. Since their gcd is 1, $\gcd(p, q) = 1$ also. Therefore, since $2pq$ is even, $p^2 - q^2$ and its factors $p + q$, $p - q$ must be odd. Also, no two of p , q , $p + q$, $p - q$ have a common prime divisor, otherwise p , q would. Then if the area $pq(p + q)(p - q)$ is a square, its factors must all be squares:

$$p = r^2, \quad q = s^2, \quad p + q = r^2 + s^2 = t^2, \quad p - q = r^2 - s^2 = u^2. \quad (1)$$

Thus the sum and difference of the squares r^2 , s^2 are also squares, so

$$r^4 - s^4 = (r^2 + s^2)(r^2 - s^2) = t^2 u^2 = v^2.$$

Therefore we should have a square number which would be equal to the sum of a square and the double of another square, while the squares of which this sum is made up would themselves have a square number for their sum.

From (1) we have

$$t^2 - u^2 = 2s^2, \quad \text{that is,} \quad t^2 = u^2 + 2s^2. \quad (2)$$

And also from (1),

$$u^2 + s^2 = r^2.$$

But if a square is made up of a square and the double of another square, its side, as I can very easily prove, is also made up of a square and the double of another square.

Since $(t + u)(t - u) = t^2 - u^2 = 2s^2$ from (2), $(t + u)(t - u)$ is even. Then one of $t + u$, $t - u$ is even, and consequently so is the other. Put

$$t + u = 2w, \quad t - u = 2x. \quad (3)$$

Then

$$s^2 = (t + u)(t - u)/2 = 2wx.$$

Tracing back through (3), (2), (1) we see that any common divisor of w , x would also be common to t , u , to t^2 , u^2 , to r^2 , s^2 , and hence to p , q . Thus w , x are relatively prime and therefore, since wx is twice a square, we have either

$$w = y^2, \quad x = 2z^2 \quad \text{or} \quad w = 2z^2, \quad x = y^2.$$

In either case,

$$t = w + x = y^2 + 2z^2. \quad (4)$$

From this we conclude that the said side is the sum of the sides about the right angle in a right-angled triangle, and that the simple square contained in the sum is the base, and the double of the other square the perpendicular.

If we let y^2 , $2z^2$ be the sides of a right triangle, then the hypotenuse h satisfies

$$\begin{aligned} h^2 &= (y^2)^2 + (2z^2)^2 = \frac{1}{2} \left((y^2 + 2z^2)^2 + (y^2 - 2z^2)^2 \right) \\ &= \frac{1}{2} (t^2 + u^2) && \text{by (3) and (4)} \\ &= r^2. && \text{by (1)} \end{aligned}$$

Hence $h = r$ and the triangle is rational.

This right-angled triangle will thus be formed from two squares, the sum and difference of which will be squares. But both these squares can be shown to be smaller than the squares originally assumed to be such that both their sum and their difference are squares.

The original squares with sum and difference equal to squares were $p = r^2$, $q = s^2$, coming from the perpendicular sides $p^2 - q^2$ and $2pq$ of the rational right triangle whose area was assumed to be a square. We now have a rational (indeed integral) right triangle with perpendicular sides y^2 , $2z^2$ whose area y^2z^2 is also a square. This triangle is smaller, since its hypotenuse r is less than side $2pq$ of the original triangle, so it gives a smaller pair of (integer) squares p' , q' , whose sum and difference are squares.

Thus, if there exist two squares such that the sum and difference are both squares, there will also exist two other integer squares which have the same property but a smaller sum. By the same reasoning we find a sum still smaller than the last found, and we can go on *ad infinitum* finding integer square numbers smaller and smaller with the same property. This is, however, impossible because there cannot be an infinite series of numbers smaller than any given integer we please.

This contradiction means that the initial assumption of a rational right triangle with square area is false. The versions of Zeuthen and Heath proceed more directly to a contradiction than Fermat by observing that the descent from the hypothetical initial triangle to the one with area y^2z^2 can be iterated to give an infinite descending sequence of integer areas. Weil (1984), p. 77, shortens the proof even further.

EXERCISES

Two of the propositions that arise in the descent from the hypothetical rational right triangle with square area are of independent interest and are also false because they imply the existence of such a triangle.

- 10.1.1** Show that the existence of squares r^2 and s^2 for which $r^2 + s^2$ and $r^2 - s^2$ are both squares implies the existence of a rational right triangle with square area.
- 10.1.2** Show that a nonzero integer solution of $r^4 - s^4 = v^2$ implies the existence of a rational right triangle with square area. (Hint: It is the same triangle as in Exercise 10.1.1.)
- 10.1.3** From Exercise 10.1.2, deduce Fermat's last theorem for $n = 4$.

The impossibility of a nonzero integer solution $r^4 - s^4 = v^2$ can also be shown by a more direct descent that avoids some of the steps used by Fermat. The main

steps are as follows, assuming r , s , and hence v have no common prime divisor.

$$\begin{aligned}
 r^4 - s^4 = v^2 &\Rightarrow r^2 = a^2 + b^2, \quad s^2 = 2ab, \quad v = a^2 - b^2 \\
 &\quad \text{for some nonzero integers } a, b \\
 &\Rightarrow a = c^2 - d^2, \quad b = 2cd \\
 &\quad \text{for some nonzero integers } c, d \\
 &\Rightarrow c = e^2, d = f^2 \text{ and } c^2 - d^2 \text{ are squares} \\
 &\quad \text{because } s^2 = 4cd(c^2 - d^2) \\
 &\quad \text{and } c, d, c^2 - d^2 \text{ have no common prime divisor} \\
 &\Rightarrow e^4 - f^4 = g^2 \\
 &\quad \text{for an integer pair } (e, f) \text{ smaller than } (r, s).
 \end{aligned}$$

10.1.4 Justify the steps in this argument.

10.2 Rational Points on Cubics of Genus 0

It is doubtful that Fermat had a proof of Fermat's last theorem because most of his work deals with curves of low degree (≤ 4), and it is highly unlikely that he could have foreseen what actually happened in the 1980s: a reduction of the n th-degree Fermat problem to a question about cubic curves. Fermat did not even talk about rational points on curves. Nevertheless, this is the most natural way to interpret his solutions of Diophantine equations and to link them with earlier and later results in the same vein by Diophantus and Euler, respectively. We have already described methods for finding rational points on curves of degree 2 (in Section 1.3) and 3 (in Section 3.5). Now we reexamine them from the point of view of *genus*, which becomes increasingly important as curves of higher degree are considered.

We cannot define genus yet (for that, see Chapters 11 and 15) but it measures the algebraic complexity of a curve. In particular, curves of genus 0 are those that can be parameterized by rational functions.

One property of a curve C of degree 2 observed in Section 1.3 is that a rational line L through a rational point P on C meets C in a second rational point, provided the equation of C has rational coefficients. Also, one obtains all rational points Q on C in this way by rotating L about C . This construction has another important consequence, not depending on the coefficients of C or L : expressing the x and y coordinates of Q in terms of the slope t of L gives a *parameterization of C by rational functions of t* (bear in mind that a rational function need not have rational coefficients).

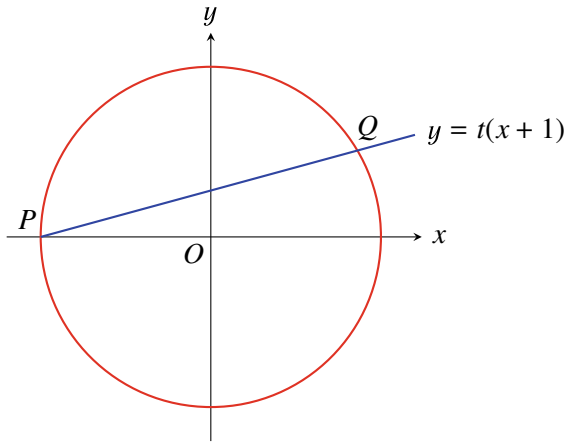


Figure 10.1: Parameterizing the circle

For example, this construction on the circle $x^2 + y^2 = 1$ in Section 1.3 gave the parameterization

$$x = \frac{1 - t^2}{1 + t^2}, \quad y = \frac{2t}{1 + t^2}$$

(Figure 10.1), which we used in Section 9.2 to find a formula for π . Genus 0 curves can be defined as those that admit parameterization by rational functions. I will now show that genus 0 includes some cubic curves by applying a similar construction to the folium of Descartes.

The folium was defined in Section 6.3 as the curve with equation

$$x^3 + y^3 = 3axy. \quad (1)$$

The origin O is an obvious rational point on the folium; moreover, O is a *double point* of the curve, as Figure 10.2 makes clear. The line $y = tx$ through O therefore meets the folium at one other point P , and varying t gives all other points P on the curve. By finding the coordinates of P as functions of t , we therefore obtain a parameterization.

To find P we substitute $y = tx$ in (1), obtaining

$$x^3 + t^3 x^3 = 3atx^2,$$

hence

$$x = \frac{3at}{1 + t^3}, \quad (2)$$

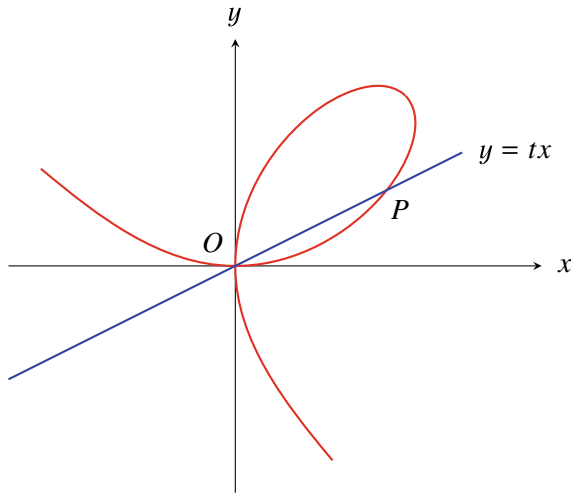


Figure 10.2: Parameterizing the folium

and therefore

$$y = \frac{3at^2}{1+t^3}. \quad (3)$$

(This derivation was implicit in Exercise 6.3.1.) A similar construction applies to any cubic with a double point, or more generally to any curve of degree $n + 1$ with an n -tuple point; hence all such curves are of genus 0.

EXERCISES

It should be noted that a double point on a curve $p(x, y) = 0$ yields a *double root* of the equation $p(x, mx + c) = 0$ for the intersections of a line $y = mx + c$ through the double point.

- 10.2.1** Observe the double root of the equation obtained by substituting $y = tx$ in equation (1) above.
- 10.2.2** Explain, using the general double root property, why a line of rational slope through a rational double point on a cubic curve with rational coefficients necessarily meets the curve at another rational point.

We note also that, as in the construction for quadratic curves, *all* rational points on the folium are obtained by this method.

- 10.2.3** Show that if x and y are rational, then so is t in (2) and (3).
- 10.2.4** Deduce from Exercise 10.2.3 that the rational points on the folium are precisely those with rational t -values.

10.3 Rational Points on Cubics of Genus 1

We cannot yet give a precise definition of genus 1, but it happens to be the genus of all cubic curves that are not of genus 0. We know from Section 10.2 that cubics of genus 1 cannot have double points, and in fact they also cannot have cusps because both these cases lead to rational parameterizations. (For one case of a cusp, see Exercise 6.4.1.) What we have yet to find are functions that do parameterize cubics of genus 1. Such functions, the *elliptic functions*, were not defined until the 19th century, and they were first used by Clebsch (1864) to parameterize cubics.

Many clues to the existence of elliptic functions were known before this, but at first they seemed to point in other directions. Initially, the mystery was how Diophantus and Fermat generated solutions of Diophantine equations. Newton's (1670s) interpretation of their results by the chord–tangent construction (Section 3.5) cleared up this first mystery—or would have if anyone had noticed it at the time. But before mathematicians really became conscious of the chord–tangent construction, they had to explain some puzzling relations between integrals of functions such as $1/\sqrt{ax^3 + bx^2 + cx + d}$, found by Fagnano (1718) and Euler (1768). Eventually Jacobi (1834) noticed that the chord–tangent construction explained this mystery too. Jacobi's explanation was cryptic, and, even though elliptic functions were then known in connection with integrals, they were not fully absorbed into number theory and the theory of curves until the appearance of Poincaré (1901).

The analytic origins of elliptic functions will be explained in the next sections. In this section we prepare to link up with this theory by deriving the algebraic relation between collinear points on a cubic curve. A much deeper treatment of the whole story appears in Weil (1984).

We start with the cubic curve equation in Newton's form (Section 6.4):

$$y^2 = ax^3 + bx^2 + cx + d. \quad (1)$$

Figure 10.3 shows this curve when $y = 0$ for three distinct real values of x .

In Section 3.5 we found that if a, b, c, d are rational, and if P_1, P_2 are rational points on the curve, then the straight line through P_1, P_2 meets the curve at a third rational point P_3 . If the equation of this straight line is

$$y = tx + k, \quad (2)$$

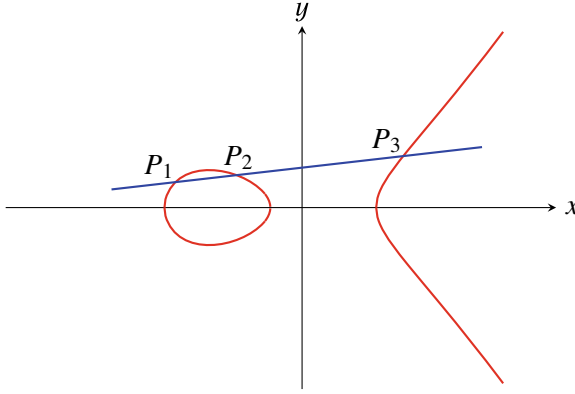


Figure 10.3: Collinear points on a cubic curve

then the result of substituting (2) in (1) is an equation

$$ax^3 + bx^2 + cx + d - (tx + k)^2 = 0 \quad (3)$$

for the x coordinates x_1, x_2, x_3 of the three points P_1, P_2, P_3 . But if the roots of (3) are x_1, x_2, x_3 its left-hand side must have the form

$$a(x - x_1)(x - x_2)(x - x_3).$$

In particular, the coefficient of x^2 must be

$$-a(x_1 + x_2 + x_3).$$

Comparing this with the actual coefficient of x^2 in (3), we find

$$b - t^2 = -a(x_1 + x_2 + x_3);$$

hence

$$x_3 = -(x_1 + x_2) - \frac{b - t^2}{a}. \quad (4)$$

If $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, then the slope $t = (y_2 - y_1)/(x_2 - x_1)$, and substituting this in (4) we finally obtain

$$x_3 = -(x_1 + x_2) - \frac{b - [(y_2 - y_1)/(x_2 - x_1)]^2}{a}, \quad (5)$$

giving x_3 as an explicit rational combination of the coordinates of P_1, P_2 . If P_1, P_2 are rational points, then (5) shows that x_3 (and hence $y_3 = tx_3 + k$) is also rational, as we already knew.

What is unexpected is that (5) is also an *addition theorem* for elliptic functions. This has the consequence that the curve can be parameterized by elliptic functions $x = f(u)$, $y = g(u)$ such that (5) is precisely the equation expressing $x_3 = f(u_1 + u_2)$ in terms of $f(u_1) = x_1$, $f(u_2) = x_2$, $g(u_1) = y_1$, and $g(u_2) = y_2$. Thus the straight-line construction of x_3 from x_1 and x_2 can also be interpreted as *addition of parameter values*, u_1 and u_2 of x_1 and x_2 . The first addition theorems were found by Fagnano (1718) and Euler (1768) by means of transformation of integrals. Euler realized that there was a connection between such transformations and number theory, but he could never quite put his finger on it. Even earlier, Leibniz had suspected such a connection when he wrote:

I . . . remember having suggested (what could seem strange to some) that the progress in our integral calculus depended in good part upon the development of that type of arithmetic which, so far as we know, Diophantus has been the first to treat systematically.

Leibniz (1702), as translated by Weil (1984)

Jacobi (1834) apparently saw the connection for the first time after receiving a volume of Euler's works on the transformation of integrals, but considerable clarification of elliptic functions was needed before Jacobi's insight became generally available. We describe some of the main steps in this process of clarification below and in Chapter 12.

EXERCISES

A proof that specific curves *cannot* be parameterized by rational functions can be modeled on Fermat's proof that $r^4 - s^4 = v^2$ is impossible in positive integers. (This is why we said in Section 10.1 that Fermat's theorem touches on elliptic curves.) The reason is that the behavior of rational functions is surprisingly similar to that of rational numbers, with polynomials playing the role of integers, and degree being the measure of size. The most convenient curve to illustrate the idea is $y^2 = 1 - x^4$, which happens to be of genus 1, hence an elliptic curve.

10.3.1 Show that a parameterization of $y^2 = 1 - x^4$ by rational functions of u implies that there are polynomials $r(u)$, $s(u)$, and $v(u)$ with

$$r(u)^4 - s(u)^4 = v(u)^2.$$

Now to imitate the rest of Fermat's proof (or the simplified version in Exercise 10.1.4) one needs a theory of divisibility for polynomials. Like the theory for

natural numbers, this can be based on the Euclidean algorithm. It follows the same basic lines as in Section 3.3, so we omit it here, but see Section 16.5 for more details.

One also needs the formula for “Pythagorean triples” of rational functions. This can be found by the geometric method of Section 1.3, carried out in the “rational function plane” where each “point” is an ordered pair $(x(u), y(u))$ of rational functions.

- 10.3.2** Convince yourself that “lines” and “slope” make sense in the rational function plane, and hence show that each point $\neq (0, -1)$ on the “unit circle”

$$x(u)^2 + y(u)^2 = 1$$

is of the form

$$x(u) = \frac{1 - t(u)^2}{1 + t(u)^2}, \quad y(u) = \frac{2t(u)}{1 + t(u)^2}$$

for some rational function $t(u)$.

- 10.3.3** Deduce from Exercise 10.3.2 a formula for “Pythagorean triples” of polynomials, like Euclid’s formula for ordinary Pythagorean triples.

It is now possible to imitate Fermat’s proof, showing that $r(u)^4 - s(u)^4 = v(u)^2$ is impossible for polynomials, and hence that $y^2 = 1 - x^4$ has no parameterization by rational functions. It follows that the same is true of certain cubic curves.

- 10.3.4** Substitute $x = (X + 1)/X$ and $y = Y/X^2$ in $y^2 = 1 - x^4$, and hence show

$$Y^2 = \text{cubic polynomial in } X.$$

Deduce that if this cubic curve in X, Y has a rational parameterization, then so has $y^2 = 1 - x^4$.

10.4 Elliptic and Circular Functions

The story of elliptic functions is one of the most curious in the history of mathematics, beginning with a complicated analytic idea—integrals of the form $\int R(t, \sqrt{p(t)}) dt$, where R is a rational function and p is a polynomial of degree 3 or 4—and reaching a climax with a simple geometric idea—the torus surface. Perhaps the best way to understand it is to compare it with a fictitious history of circular functions that begins with the integral $\int dt/\sqrt{1-t^2}$ and ends with the discovery of the circle. Unlikely as this fiction is, it was paralleled by the actual development of elliptic functions between the 1650s and the 1850s.

The late recognition of the geometric nature of elliptic functions was due to late recognition of the existence and geometric nature of complex numbers. In fact, the later history of elliptic functions unfolds alongside

the development of complex numbers, which is the subject of Chapter 12. In the present chapter we are concerned mainly with the history up to 1800, before complex numbers entered in a really essential way. However, there are some subplots of the main story that do not require complex numbers for their understanding and nicely show the parallel with the fictitious history of circular functions. It is convenient to relate one of these now, because it illustrates the parallel in a simplified way and also ties up a loose end from Section 10.3—the parameterization of cubic curves.

Parameterization of Cubic Curves

To see how to construct parameterizing functions for a cubic curve, we first reconstruct the parameterizing functions

$$\begin{aligned}x &= \sin u, \\y &= \cos u\end{aligned}$$

for the circle $x^2 + y^2 = 1$, pretending that we do not know this curve geometrically but only as an algebraic relation between x and y .

The sine function can be defined as the inverse f of $f^{-1}(x) = \sin^{-1} x$, which in turn is definable as the integral

$$f^{-1}(x) = \int_0^x \frac{dt}{\sqrt{1-t^2}}.$$

Finally, the integral can be related to the equation $y^2 = 1 - x^2$, because the integrand $1/\sqrt{1-x^2}$ is simply $1/y$. Why do we use this integrand rather than any other to define $u = f^{-1}(x)$ and hence obtain x as a function $f(u)$? The answer is that we then obtain y as $f'(u)$; hence x, y are both functions of the parameter u . This is confirmed by the calculations:

$$f'(u) = \frac{dx}{du} = 1 \Big/ \frac{du}{dx}$$

and

$$\frac{du}{dx} = \frac{d}{dx} \int_0^x \frac{dt}{\sqrt{1-t^2}} = \frac{1}{\sqrt{1-x^2}} = \frac{1}{y};$$

so $y = f'(u)$ (which of course is $\cos u$).

Exactly the same construction can be used to parameterize any relation of the form $y^2 = p(x)$. We put

$$u = g^{-1}(x) = \int_0^x \frac{dt}{\sqrt{p(t)}}$$

to get $x = g(u)$, and then find that $y = g'(u)$ by differentiation of u . Thus in a sense it is trivial to parameterize curves of the form $y^2 = p(x)$ (which we know from Section 7.4 to include all cubic curves, up to a projective transformation of x and y). As we will see in the next section, the integrals $\int dt/\sqrt{p(t)}$ had been studied since the 1600s for p a polynomial of degree 3 or 4; however, no one thought to invert them until about 1800. Jacobi had a deep knowledge of both the integrals *and* inversion when he wrote his cryptic paper, Jacobi (1834), pointing out the relation between integrals and rational points on curves (Sections 10.3 and 10.7). Thus it seems likely he understood the preceding parameterization, though such a parameterization was first given explicitly by Clebsch (1864).

EXERCISES

It may happen that the integral $\int_0^x dt/\sqrt{p(t)}$ does not converge because of the behavior of $1/\sqrt{p(t)}$ at $t = 0$. But in that case one can use the parameter $u = f^{-1}(x) = \int_a^x dt/\sqrt{p(t)}$ for some other value of a .

10.4.1 Check that $y = f'(u)$ remains true with this change of definition.

When the cubic curve is $y^2 = x^3$, which has a rational parameterization, the parameterizing functions constructed above indeed turn out to be rational.

10.4.2 Given $y = x^{3/2}$, find $x = f(u)$ and $y = f'(u)$, where $u = f^{-1}(x) = \int_a^x \frac{dt}{t^{3/2}}$.

10.5 Elliptic Integrals

Integrals of the form $\int R(t, \sqrt{p(t)}) dt$, where R is a rational function and p is a polynomial of degree 3 or 4 without multiple factors, are called *elliptic integrals*, because the first example occurs in the formula for the arc length of the ellipse. (The functions obtained by inverting elliptic integrals are called *elliptic functions*, and the curves that require elliptic functions for their parameterization are called *elliptic curves*. This drift in the meaning of “elliptic” is rather unfortunate because the ellipse, being parameterizable by rational functions, is not an elliptic curve!)

Elliptic integrals arise in many important problems of geometry and mechanics, for example, finding arc lengths of the ellipse and hyperbola, period of the simple pendulum, and deflection of a thin elastic bar. See for example, Melzak (1976), pp. 253–269. When these problems first arose in the late 17th century they were the first obstacle to Leibniz’s program of integration in “closed form” or “by elementary functions.” As mentioned

in Section 8.6, Leibniz thought the proper solution of an integration problem $\int f(x) dx$ was a known function $g(x)$ with the property $g'(x) = f(x)$. The functions then “known,” and now called “elementary,” were those composed from algebraic, circular, and exponential functions and their inverses.

All efforts to express elliptic integrals in these terms failed, and as early as 1694 Jakob Bernoulli conjectured that the task was impossible. The conjecture was eventually confirmed by Liouville (1833), in the course of showing that a large class of integrals is nonelementary. In the meantime, mathematicians had discovered so many properties of elliptic integrals, and the elliptic functions obtained from them by inversion, that they could be considered known even if not elementary.

The key that unlocked many of the secrets of elliptic integrals was the curve known as the *lemniscate of Bernoulli* (Figure 10.4). This curve was mentioned briefly in Section 2.5 as one of the spiric sections of Perseus.

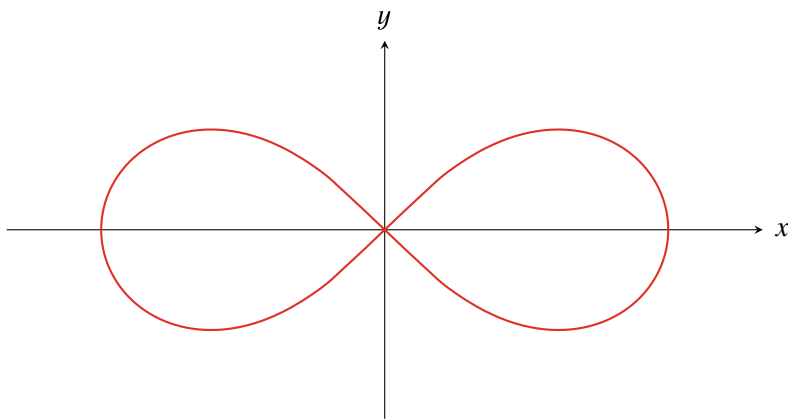


Figure 10.4: The lemniscate of Bernoulli

It has cartesian equation

$$(x^2 + y^2)^2 = x^2 - y^2$$

and polar equation

$$r^2 = \cos 2\theta.$$

The first to consider it in its own right was Jakob Bernoulli (1694). He showed that its arc length is the elliptic integral $\int_0^x dt / \sqrt{1 - t^4}$, later known as the *lemniscatic integral*, thus giving this formal expression a concrete

geometric interpretation. Many later developments in the theory of elliptic integrals and functions grew from interplay between the lemniscate and the lemniscatic integral. As the simplest elliptic integral, or at any rate the most analogous to the arcsine integral $\int_0^x dt/\sqrt{1-t^2}$, the lemniscatic integral $\int_0^x dt/\sqrt{1-t^4}$ was the most amenable to manipulation. It was often possible, after some property had been proved for the lemniscatic integral, to extend the argument to more general elliptic integrals.

The most notable example of this methodology was in the discovery of the addition theorems, which we discuss in the next section.

EXERCISES

The properties of the lemniscate mentioned above are easily proved by some standard analytic geometry and calculus.

10.5.1 Deduce the cartesian equation of the lemniscate from its polar equation

$$r^2 = \cos 2\theta.$$

10.5.2 Use the polar equation of the lemniscate and the formula for the element of arc in polar coordinates,

$$ds = \sqrt{(r d\theta)^2 + dr^2}$$

to deduce that arc length of the lemniscate is given by

$$s = \int \frac{d\theta}{r}.$$

10.5.3 Conclude, by changing the variable of integration to r , that the total length of the lemniscate is $4 \int_0^1 dr/\sqrt{1-r^4}$.

Unlike the arcsine integrand $1/\sqrt{1-t^2}$, which is rationalized by substituting $2v/(1+v^2)$ for t , the lemniscatic integrand $1/\sqrt{1-t^4}$ cannot be rationalized by replacing t by any rational function.

10.5.4 Explain how this follows from the exercises in Section 10.3.

It was this connection between the lemniscatic integral and Fermat's theorem on the impossibility of $r^4 - s^4 = v^2$ in positive integers that led Jakob Bernoulli to suspect the impossibility of evaluating the lemniscatic integral by known functions.

10.6 Doubling the Arc of the Lemniscate

An addition theorem is a formula expressing $f(u_1 + u_2)$ in terms of $f(u_1)$ and $f(u_2)$, and perhaps also $f'(u_1)$ and $f'(u_2)$. For example, the addition theorem for the sine function is

$$\sin(u_1 + u_2) = \sin u_1 \cos u_2 + \sin u_2 \cos u_1.$$

Since the derivative, $\cos u$, of $\sin u$ equals $\sqrt{1 - \sin^2 u}$, we can also write the addition theorem as

$$\sin(u_1 + u_2) = \sin u_1 \sqrt{1 - \sin^2 u_2} + \sin u_2 \sqrt{1 - \sin^2 u_1},$$

showing that $\sin(u_1 + u_2)$ is an algebraic function of $\sin u_1$ and $\sin u_2$.

To simplify the comparison with elliptic functions we consider the following special case of the sine addition theorem:

$$\sin 2u = 2 \sin u \sqrt{1 - \sin^2 u}. \quad (1)$$

If we let

$$u = \sin^{-1} x = \int_0^x \frac{dt}{\sqrt{1 - t^2}},$$

then

$$2u = 2 \int_0^x \frac{dt}{\sqrt{1 - t^2}}.$$

But from (1) we also have

$$2u = \sin^{-1}(2x \sqrt{1 - x^2}),$$

so

$$2 \int_0^x \frac{dt}{\sqrt{1 - t^2}} = \int_0^{2x \sqrt{1 - x^2}} \frac{dt}{\sqrt{1 - t^2}}. \quad (2)$$

Bearing in mind that $\sin^{-1} x = \int_0^x dt / \sqrt{1 - t^2}$ represents the angle u seen in Figure 10.5, equation (2) tells us that the angle (or arc length) u is doubled by going from x to $2x \sqrt{1 - x^2}$. The latter number, since it is obtained from x by rational operations and square roots, is constructible from x by ruler and compass (confirming the geometrically obvious fact that an angle can be duplicated by ruler and compass).

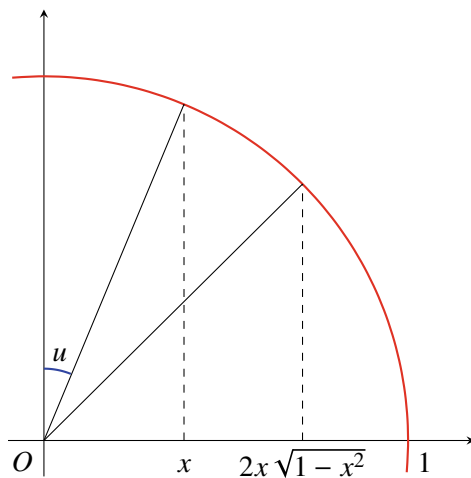


Figure 10.5: Doubling a circular arc

All this has a remarkable parallel in the properties of the lemniscate and its arc-length integral $\int_0^x dt/\sqrt{1-t^4}$. The discovery of a formula for doubling the arc of the lemniscate by Fagnano (1718) showed that geometric information could be extracted from the previously intractable elliptic integrals, and we can also view it as the first step toward the theory of elliptic functions. In our notation, Fagnano's formula is

$$2 \int_0^x \frac{dt}{\sqrt{1-t^4}} = \int_0^{2x\sqrt{1-x^4}/(1+x^4)} \frac{dt}{\sqrt{1-t^4}}. \quad (3)$$

Since $2x\sqrt{1-x^4}/(1+x^4)$ is obtained from x by rational operations and square roots, (3) shows, like (2), that the arc can be doubled by ruler and compass construction.

EXERCISES

Fagnano derived his formula by two substitutions that, as Siegel (1969), p. 3, points out, are analogous to a natural substitution for the arcsine integral. The following exercises compare the effect of the substitution $t = 2v/(1+v^2)$ in $dt/\sqrt{1-t^2}$ with analogous substitutions for t^2 in $dt/\sqrt{1-t^4}$.

10.6.1 Show that substituting $t = 2v/(1+v^2)$ gives $\sqrt{1-t^2} = (1-v^2)/(1+v^2)$ and hence that $dt/\sqrt{1-t^2} = 2dv/(1+v^2)$.

10.6.2 Show that $t^2 = 2v^2/(1 + v^4)$ gives $\sqrt{1 - t^4} = (1 - v^4)/(1 + v^4)$ and hence

$$\frac{dt}{\sqrt{1 - t^4}} = \sqrt{2} \frac{dv}{\sqrt{1 + v^4}}.$$

It follows that this change of variable corresponds to a certain relation between integrals, which turns out to be half way to the Fagnano formula.

10.6.3 Deduce from Exercise 10.6.2 that

$$\sqrt{2} \int_0^x \frac{dv}{\sqrt{1 + v^4}} = \int_0^{\sqrt{2}x/\sqrt{1+x^4}} \frac{dt}{\sqrt{1 - t^4}}.$$

To complete the journey to the Fagnano formula we make a second, similar, substitution that recreates the lemniscatic integral.

10.6.4 Similarly show that the substitution $v^2 = 2w^2/(1 - w^4)$ gives

$$\frac{dv}{\sqrt{1 + v^4}} = \sqrt{2} \frac{dw}{\sqrt{1 - w^4}}.$$

10.6.5 Check that the result of the substitutions in Exercises 10.6.2 and 10.6.4 is

$$t = \frac{2w \sqrt{1 - w^4}}{1 + w^4}$$

and that the corresponding relation between integrals is the Fagnano duplication formula.

10.7 General Addition Theorems

The Fagnano duplication formula was a little-known curiosity until Euler received a copy of Fagnano's works on December 23, 1751, a date later described by Jacobi as "the birth day of the theory of elliptic functions." Euler was the first to see that Fagnano's substitution trick was not just a curious fluke but a revelation of the behavior of elliptic integrals. With his superb manipulative skill Euler was quickly able to extend it to very general addition theorems; first to the addition theorem for the lemniscatic integral,

$$\int_0^x \frac{dt}{\sqrt{1 - t^4}} + \int_0^y \frac{dt}{\sqrt{1 - t^4}} = \int_0^{(x \sqrt{1-y^4} + y \sqrt{1-x^4})/(1+x^2y^2)} \frac{dt}{\sqrt{1 - t^4}};$$

then to $\int dt/\sqrt{p(t)}$, where $p(t)$ is an arbitrary polynomial of degree 4. An ingenious reconstruction of Euler's train of thought, by analogy with the

arcsine addition theorem

$$\int_0^x \frac{dt}{\sqrt{1-t^2}} + \int_0^y \frac{dt}{\sqrt{1-t^2}} = \int_0^{x\sqrt{1-y^2}+y\sqrt{1-x^2}} \frac{dt}{\sqrt{1-t^2}},$$

has been given by Siegel (1969), pp. 1–10. Of course, Euler was dealing only with elliptic integrals, *not* with elliptic functions. But Jacobi could see his results as addition theorems for elliptic functions as easily as we can see that the arcsine addition theorem is really a theorem about sines!

It should be mentioned that Euler's addition theorems do not cover all kinds of elliptic integrals. The classical theory of elliptic integrals of the different kinds, with their various addition and transformation theorems, was systematized by Legendre (1825). Ironically, this was just before the appearance of elliptic functions, which made much of Legendre's work obsolete.

These early investigations exploited some of the formal similarities between $\int dt/\sqrt{p(t)}$, where p is a polynomial of degree 4, and $\int dt/\sqrt{q(t)}$, where q is a quadratic. There is no real difference if p is of degree 3, as an easy transformation shows (Exercise 10.7.1). This is why $\int dt/\sqrt{p(t)}$ is also called an elliptic integral when p is of degree 3. In fact, it eventually turned out that the most convenient integral to use as a basis for the theory of elliptic functions is $\int dt/\sqrt{4t^3 - g_2t - g_3}$, whose inverse is known as the Weierstrass \wp -function.

The addition theorem for this integral is

$$\int_0^{x_1} \frac{dt}{\sqrt{4t^3 - g_2t - g_3}} + \int_0^{x_2} \frac{dt}{\sqrt{4t^3 - g_2t - g_3}} = \int_0^{x_3} \frac{dt}{\sqrt{4t^3 - g_2t - g_3}},$$

where x_3 is none other than the x -coordinate of the third point on

$$y^2 = 4x^3 - g_2x - g_3$$

of the straight line through (x_1, y_1) and (x_2, y_2) (see Section 10.3). Now that we know, from Section 10.4, that this curve is parameterized by $x = \wp(u)$, $y = \wp'(u)$, defined by inverting the integral, some connection between the geometry of the curve and the addition theorem is understandable. But the stunning simplicity of the relationship seems to demand a deeper explanation. This lies in the realm of complex numbers, which we enter briefly in the next section and more thoroughly in Chapter 12.

EXERCISES

10.7.1 Show that the substitution $t = 1/u$ transforms

$$\frac{dt}{\sqrt{(t-a)(t-b)(t-c)}} \quad \text{into} \quad \frac{-du}{\sqrt{u(1-ua)(1-ub)(1-uc)}}.$$

Conversely, we can transform quartic polynomials under the square root sign to cubics, even in cases where the quartic is not of the form obtained in Exercise 10.5.1.

10.7.2 Transform

$$\frac{dt}{\sqrt{1-t^4}} \quad \text{into} \quad \frac{du}{\sqrt{\text{cubic polynomial in } u}}$$

by making a suitable substitution for t .

10.8 Elliptic Functions

The idea of inverting elliptic integrals to obtain elliptic functions is due to Gauss, Abel, and Jacobi. Gauss had the idea in the late 1790s but did not publish it; Abel had the idea in 1823 and published it in 1827, independently of Gauss. Jacobi seems to have been approaching the idea of inversion in 1827, but was stung into action only by the appearance of Abel's paper. His ideas then developed at an explosive rate, and he published the first book on elliptic functions, the *Fundamenta nova theoriae functionum ellipticarum*, two years later (Jacobi (1829)).

Gauss first considered inverting an elliptic integral in 1796, in the case of $\int dt/\sqrt{1-t^3}$. The next year he inverted the lemniscatic integral and made more progress. Defining the *lemniscatic sine function* $x = sl(u)$ by

$$u = \int_0^x \frac{dt}{\sqrt{1-t^4}},$$

he found that this function is periodic, like the sine, with period

$$2\varpi = 4 \int_0^1 \frac{dt}{\sqrt{1-t^4}}.$$

He also noticed that $sl(u)$ invites complex arguments, since $i^2 = -1$ implies

$$\frac{d(it)}{\sqrt{1-(it)^4}} = i \frac{dt}{\sqrt{1-t^4}};$$

so $sl(iu) = isl(u)$ and the lemniscatic sine has a second period $2i\varpi$. Thus Gauss discovered *double periodicity*, a key property of the elliptic functions, though at first he did not realize its significance. The scope and importance of elliptic functions hit him on May 30, 1799, when he found an extraordinary numerical coincidence. His diary entry of that day reads:

We have established that the arithmetic–geometric mean between 1 and $\sqrt{2}$ is π/ϖ to 11 places; the demonstration of this fact will surely open up an entirely new field of analysis.

Gauss had been fascinated by the arithmetic–geometric mean (agM) since 1791, when he was 14. The $\text{agM}(a, b)$ of two positive numbers a and b is the common limit of the two sequences $\{a_n\}$ and $\{b_n\}$ defined by

$$\begin{aligned} a_0 &= a, & b_0 &= b, \\ a_{n+1} &= \frac{a_n + b_n}{2}, & b_{n+1} &= \sqrt{a_n b_n}. \end{aligned}$$

For more information on its theory and history, see Cox (1984).

It is indeed true that $\text{agM}(1, \sqrt{2}) = \pi/\varpi$, as Gauss soon proved, and the “entirely new field of analysis” he created from the stew of these ideas was extraordinarily rich. It encompassed elliptic functions in general, the theta functions later rediscovered by Jacobi, and the modular functions later rediscovered by Klein. The theory was not significantly improved until the 1850s, when Riemann showed that double periodicity becomes obvious when elliptic integrals are placed in a suitable geometric setting.

Unfortunately, Gauss released virtually none of his results on elliptic functions. Apart from a formula for $\text{agM}(a, b)$ as an elliptic integral (Gauss (1818)), he published nothing until Abel’s results appeared in 1827—then promptly claimed them as his own. He wrote to Bessel (Gauss (1828)):

I shall most likely not soon prepare my investigations on the transcendental functions which I have had for many years—since 1798. ... Herr Abel has now, as I see, anticipated me and relieved me of the burden in regard to one third of these matters.

It was disingenuous of Gauss to claim he had more results than Abel, because Abel also had results unknown to Gauss. True, Gauss had priority on the key ideas of inversion and double periodicity, but priority isn’t everything, as Gauss himself perhaps knew. His own cherished discovery of the relation between agM and elliptic integrals had not only been found earlier, but even published by Lagrange (1785).

A Postscript on the Lemniscate

The duplication of the arc of the lemniscate had some interesting consequences for the lemniscate itself. Fagnano showed, by similar arguments, that a quadrant of the lemniscate can be divided into two, three, or five equal arcs by ruler and compass (see Ayoub (1984)). This raised a question: for which n can the lemniscate be divided into n equal parts by ruler and compass? Recall from Section 2.3 that the corresponding question for the circle had been answered by Gauss (1801), Art. 366. As mentioned in there, the answer is $n = 2^m p_1 p_2 \cdots p_k$, where the p_i are distinct primes of the form $2^{2^h} + 1$. In the introduction to his theory (Art. 355), Gauss claims:

The principles of the theory which we are going to explain actually extend much further than we will indicate. For they can be applied not only to circular functions but just as well to other transcendental functions, e.g. to those which depend on the integral $\int (1/\sqrt{1-x^4}) dx$.

However, his surviving papers do not include any result on the lemniscate as incisive as his result on the circle. There is only a diary entry of March 21, 1797, stating divisibility of the lemniscate into five equal parts.

The answer to the problem of dividing the lemniscate into n equal parts was found by Abel (1827), transforming Gauss's obscurity into crystal clarity: division by ruler and compass is possible for *precisely the same* n as for the circle. This wonderful result serves, perhaps better than any other, to underline the unifying role of elliptic functions in geometry, algebra, and number theory. A modern proof of it may be found in Rosen (1981).

EXERCISES

The following exercises show how the lemniscatic sine and its derivative are quite analogous to the ordinary sine and its derivative, the cosine.

10.8.1 Show that $sl'(u) = \sqrt{1 - sl^4(u)}$.

10.8.2 Deduce from the Euler addition theorem (Section 10.7) that

$$sl(u+v) = \frac{sl(u)sl'(v) + sl(v)sl'(u)}{1 + sl^2(u)sl^2(v)}.$$



11

Complex Numbers and Curves

PREVIEW

This chapter revisits polynomial equations and algebraic curves, observing how these topics are simplified by introducing complex numbers. That's right: the so-called “complex” numbers actually make things simpler.

One of the reasons for the simplifying power of complex numbers is their two-dimensional nature. The extra dimension gives more room for solutions of equations to exist. For example, the equation $x^n = 1$, which has only one or two solutions in the real numbers, has n different solutions in the complex numbers, equally spaced around the unit circle.

In fact, any equation of degree n has n complex solutions, when solutions are properly counted. This is the *fundamental theorem of algebra*, and it follows from intuitively simple properties of the plane and continuous functions.

The fundamental theorem also enables us to get the “right” number of intersections between a curve of degree m and a curve of degree n . However, it is not enough to introduce complex coordinates: getting the right count of intersections also requires us to adjust our viewpoint in two other ways: by counting intersections according to their *multiplicity*, and by counting points *at infinity*.

For these reasons, and others, algebraic geometry moved to the setting of complex projective space in the 19th century. In this chapter we see how this affects our view of algebraic curves: in short, they become *surfaces*.

11.1 Impossible Numbers

In previous chapters it has often been claimed that certain mysteries—de Moivre’s formula for $\sin n\theta$ (Section 5.6), factorization of polynomials (Section 5.7), classification of cubic curves (Section 7.4), and the behavior of elliptic functions (Section 10.8)—are cleared up by the introduction of complex numbers. That complex numbers do all this and more is one of the miracles of mathematics. At the beginning of their history, complex numbers $a + b\sqrt{-1}$ were considered to be “impossible numbers,” tolerated only because they seemed useful for solving cubic equations. But their significance turned out to be geometric and ultimately led to the unification of algebra with an enriched domain of geometry, including topology and another “impossible” field, non-Euclidean geometry.

In this chapter we will see how complex numbers emerged from the theory of equations and enabled its fundamental theorem to be proved—at which point it became clear that complex numbers had meaning far beyond algebra. Their impact on curves and function theory is described later in this chapter and in the next. Non-Euclidean geometry had entirely different origins but arrived at the same place as complex function theory in the 1880s, thanks to complex numbers. This unexpected meeting is described in Chapter 13.

Quadratic Equations

In theory, mathematics first calls on complex numbers to solve certain quadratic equations, such as the equation $x^2 + 1 = 0$. However, this did not happen when quadratic equations first appeared, since at that time there was no *need* for all quadratic equations to have solutions. Many quadratic equations are implicit in Greek geometry, but one does not demand that every geometric problem have a solution. If one asks whether a particular circle and line intersect, say, then the answer can be yes or no. If yes, the quadratic equation for the intersection has a solution; if no, it has no solution. An “imaginary solution” is uncalled for in this context.

Even when quadratic equations appeared in pure algebra, with Diophantus and the Arab mathematicians, there was initially no reason for complex solutions. One only wanted to know whether there were real solutions, and if not the answer was simply—no solution. This is the appropriate answer when quadratics are solved by geometrically completing the square (Section 5.3), as was done up to the time of Cardano. A square of

negative area did not exist in geometry. The story might have been different had mathematicians used symbols more and dared to consider the symbol $\sqrt{-1}$ as an object in its own right, but this did not happen until quadratics had been overtaken by cubics, at which stage complex numbers became unavoidable, as we will now see.

11.2 Cubic Equations

The del Ferro–Tartaglia–Cardano solution of the cubic equation

$$y^3 = py + q$$

is

$$y = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}} + \sqrt[3]{\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}}$$

as we saw in Section 5.5. We notice that it involves complex numbers when $(q/2)^2 - (p/3)^3 < 0$. However, one cannot dismiss this as a case with no solution, *because a cubic always has at least one real root* (since $y^3 - py - q$ is positive for large positive y and negative for large negative y). Thus the Cardano formula raises the problem of reconciling a real value, found by inspection, say, with an expression of the form

$$\sqrt[3]{a + b\sqrt{-1}} + \sqrt[3]{a - b\sqrt{-1}}$$

Cardano did not face up to this problem in his *Ars magna* (1545). He did, it is true, once mention complex numbers, but in connection with a quadratic equation and accompanied by the comment that these numbers were “as subtle as they are useless” (Cardano (1545), Ch. 37, Rule II).

The first to take complex numbers seriously and use them to achieve the necessary reconciliation was Bombelli (1572). Bombelli worked out the formal algebra of complex numbers, with the particular aim of reducing expressions $\sqrt[3]{a + b\sqrt{-1}}$ to the form $c + d\sqrt{-1}$. His method enabled him to show the reality of some expressions resulting from Cardano’s formula. For example, the solution of

$$x^3 = 15x + 4$$

is

$$x = \sqrt[3]{2 + 11\sqrt{-1}} + \sqrt[3]{2 - 11\sqrt{-1}}$$

according to the formula. On the other hand, inspection gives the solution $x = 4$. Bombelli had the hunch that the two parts of x in the Cardano formula were of the form $2 + n\sqrt{-1}$ and $2 - n\sqrt{-1}$. He found, by cubing these expressions formally [using $(\sqrt{-1})^2 = -1$, and $n = 1$], that indeed

$$\sqrt[3]{2 + 11\sqrt{-1}} = 2 + \sqrt{-1},$$
$$\sqrt[3]{2 - 11\sqrt{-1}} = 2 - \sqrt{-1},$$

hence the Cardano formula also gives their sum $x = 4$.

Figure 11.1 is a facsimile of the manuscript page on which Bombelli stated his result: *Somma 4*. The figure is from a 1569 version of Bombelli’s *L’Algebra*: page 72 verso in codice B. 1569, which is in the Biblioteca dell’ Archiginnasio in Bologna, and is used with their permission. It was transcribed from Bombelli’s lectures by F. M. Salando.

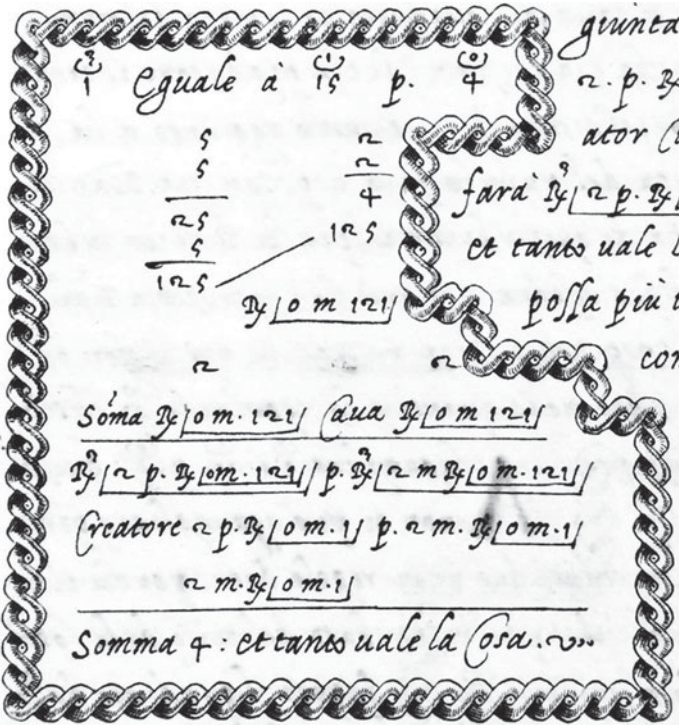


Figure 11.1: Bombelli’s manuscript

He has placed the problem and its solution inside a decorative border. It has the equation $x^3 = 15x + 4$ at the top (in his notation, which does not show the variable x —only its coefficients and, directly above them, its exponents), and the conclusion $(2 + \sqrt{-1}) + (2 - \sqrt{-1}) = 4$ at the bottom. Bombelli includes the trivial calculations of $5 \times 5 \times 5 = 125$ and $2 \times 2 = 4$, needed for the Cardano formula. But he does *not* include the crucial calculation of $(2 + \sqrt{-1})^3$ needed to remove the cube roots—he simply removes them without explanation!

It is not hard to pick out the preceding expressions when one allows for the notation and the fact that $11\sqrt{-1}$ is written as $\sqrt{0 - 121}$. Note in particular the sign R for “root,” which today is still in use by pharmacists (presumably because of the roots once common for medical purposes).

Much later, Hölder (1896) showed that any algebraic formula for the solution of the cubic must involve square roots of quantities that become negative for particular values of the coefficients. A proof of Hölder’s result may be found in van der Waerden (1949), p. 180.

EXERCISES

11.2.1 Check that $(2 + \sqrt{-1})^3 = 2 + 11\sqrt{-1}$.

It is possible to work backwards and concoct a cubic equation with an obvious solution that can be reconciled with the hideous solution in the Cardano formula. Here is an example.

11.2.2 Check that $(3 + \sqrt{-1})^3 = 18 + 26\sqrt{-1}$.

11.2.3 Hence explain why

$$6 = (3 + \sqrt{-1}) + (3 - \sqrt{-1}) = \sqrt[3]{18 + 26\sqrt{-1}} + \sqrt[3]{18 - 26\sqrt{-1}}.$$

11.2.4 Find p and q such that

$$18 = \frac{q}{2} \quad \text{and} \quad 26\sqrt{-1} = \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}.$$

11.2.5 Check that 6 is a solution of the equation $x^3 = px + q$ for the values of p and q found in Exercise 11.2.4.

11.3 Angle Division

In Section 5.6 we saw how Viète related angle trisection to the solution of cubic equations, and how Leibniz (1675) and de Moivre (1707) solved the

angle n -section equation by the Cardano-type formula

$$x = \frac{1}{2} \sqrt[n]{y + \sqrt{y^2 - 1}} + \frac{1}{2} \sqrt[n]{y - \sqrt{y^2 - 1}}. \quad (1)$$

We also saw how this and Viète's formulas for $\cos n\theta$ and $\sin n\theta$ could easily be explained by the formula

$$(\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta \quad (2)$$

usually associated with de Moivre. Actually, de Moivre never stated (2) explicitly. The closest he came was to give a formula for $(\cos \theta + i \sin \theta)^{1/n}$ in de Moivre (1730). (See Smith (1959) for a series of extracts from the work of de Moivre on angle division). It seems that the clues in the algebra of circular functions were not strong enough to reveal (2) until a deeper reason for it had been brought to light by calculus.

Complex numbers made their entry into the theory of circular functions in a paper on integration by Johann Bernoulli (1702). Observing that $\sqrt{-1} = i$ makes possible the partial fraction decomposition

$$\frac{1}{1+z^2} = \frac{1/2}{1+zi} + \frac{1/2}{1-zi},$$

Bernoulli saw that integration would give an expression for $\tan^{-1} z$ as an imaginary logarithm, though he did not write down the expression in question and was evidently puzzled as to what it could mean. In Section 12.1 we will see how Euler clarified Johann Bernoulli's discovery and developed it into the beautiful theory of complex logarithms and exponentials. What is relevant here is that Johann Bernoulli (1712) took up the idea again, and this time he carried out the integration to obtain an algebraic relation between $\tan n\theta$ and $\tan \theta$. His argument is as follows. Given

$$y = \tan n\theta, \quad x = \tan \theta,$$

we have

$$n\theta = \tan^{-1} y = n \tan^{-1} x;$$

hence, taking differentials gives

$$\frac{dy}{1+y^2} = \frac{n dx}{1+x^2},$$

or

$$dy \left(\frac{1}{y+i} - \frac{1}{y-i} \right) = n dx \left(\frac{1}{x+i} - \frac{1}{x-i} \right).$$

Integration gives

$$\log(y+i) - \log(y-i) = n \log(x+i) - n \log(x-i),$$

that is,

$$\log \frac{y+i}{y-i} = \log \left(\frac{x+i}{x-i} \right)^n,$$

whence

$$(x-i)^n(y+i) = (x+i)^n(y-i). \quad (3)$$

This formula was the first of the de Moivre type actually to use i explicitly and the first example of a phenomenon later articulated by Hadamard (1954), Chapter VIII:

the shortest and best way between two truths in the real domain often passes through the imaginary one.

Solving (3) for y as a function of x expresses $\tan n\theta$ as a rational function of $\tan \theta$, which is difficult to obtain using real formulas alone. In fact, it is easy to show from (3) that y is the quotient of the polynomials consisting of alternate terms in $(x+1)^n$, provided with alternate $+$ and $-$ signs (see exercises).

18th-century mathematicians had mixed feelings about $\sqrt{-1}$. They were willing to use it en route to results about real numbers but doubted that it had a concrete meaning of its own. Cotes (1714) even used $a + \sqrt{-1}b$ to represent the point (a, b) in the plane (as Euler did later), apparently without noticing that (a, b) was a valid *interpretation* of $a + \sqrt{-1}b$. Since results about $\sqrt{-1}$ were suspect, they were often left unstated when it was possible to state an equivalent result about reals. This may explain why de Moivre stated (1) but not (2). Another example of the avoidance of results about $\sqrt{-1}$ is the remarkable theorem on the regular n -gon discovered by Cotes in 1716 and published posthumously in Cotes (1722):

If A_0, \dots, A_{n-1} are equally spaced points on the unit circle with center O , and if P is a point on OA_0 such that $OP = x$, then (Figure 11.2)

$$PA_0 \cdot PA_1 \cdots PA_{n-1} = 1 - x^n.$$

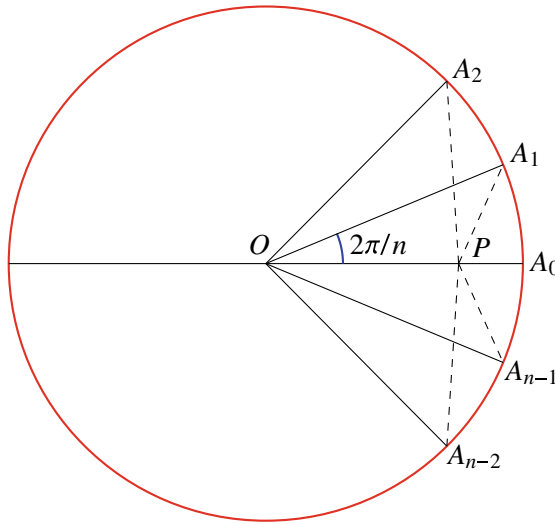


Figure 11.2: Cotes's theorem

This theorem not only relates the regular n -gon to the polynomial $x^n - 1$ but in fact geometrically realizes the *factorization of $x^n - 1$ into real linear and quadratic factors*. By symmetry one has $PA_1 = PA_{n-1}, \dots$, so

$$PA_0 \cdot PA_1 \cdots PA_{n-1} = \begin{cases} PA_0 \cdot PA_1^2 \cdot PA_2^2 \cdots PA_{(n-1)/2}^2 & n \text{ odd,} \\ PA_0 \cdot PA_1^2 \cdot PA_2^2 \cdots PA_{n/2-1}^2 PA_{n/2} & n \text{ even.} \end{cases}$$

$PA_0 = 1 - x$ is a real linear factor, as is $PA_{n/2}$ when n is even, and it follows from the cosine rule in triangle OPA_k that

$$PA_k^2 = 1 - 2x \cos \frac{2k\pi}{n} + x^2.$$

The easiest route from here to the theorem is by splitting PA_k^2 into complex linear factors and using de Moivre's theorem. We can only speculate that this was Cotes's method, since he stated his theorem without proof. The theorem has a second half which similarly decomposes $1 + x^n$ into real linear and quadratic factors. These factorizations were needed to integrate $1/(1 \pm x^n)$ by resolution into partial fractions, which was Cotes's main objective. Such problems were then high on the mathematical agenda, and they motivated research into the factorization of polynomials, in particular the first attempts to prove the fundamental theorem of algebra.

EXERCISES

Johann Bernoulli's formula relating $y = \tan n\theta$ to $x = \tan \theta$ is false for some values of n , because it neglects a possible constant of integration. The result of integration should be

$$\log(y + i) - \log(y - i) = n \log(x + i) - n \log(x - i) + C,$$

for some C , leading to

$$\frac{y + i}{y - i} = D \frac{(x + i)^n}{(x - i)^n}, \quad (*)$$

for some constant D (equal to e^C). Sometimes $D = 1$ gives the correct formula, but sometimes we need $D = -1$.

11.3.1 Show that $D = 1$ gives the correct formula when $n = 1$.

11.3.2 Using formulas for $\sin 2\theta$ and $\cos 2\theta$, or otherwise, show that

$$\tan 2\theta = \frac{2 \tan \theta}{1 - \tan^2 \theta},$$

and check that this follows from (*) for $D = -1$, but not for $D = 1$.

11.3.3 Use the formula in Exercise 11.3.2 to express $\tan 4\theta$ in terms of $\tan 2\theta$, and hence in terms of $\tan \theta$.

11.3.4 Letting $y = \tan 4\theta$ and $x = \tan \theta$, express the result of Exercise 11.3.3 as

$$y = \frac{4x - 4x^3}{x^4 - 6x^2 + 1},$$

and check that this follows from (*) when $D = -1$.

11.4 The Fundamental Theorem of Algebra

The fundamental theorem of algebra is the statement that every polynomial equation $p(z) = 0$ has a solution in the complex numbers. As Descartes observed (Section 5.7), a solution $z = a$ implies that $p(z)$ has a factor $z - a$. The quotient $q(z) = p(z)/(z - a)$ is then a polynomial of lower degree; hence if every polynomial equation has a solution, we can also extract a factor from $q(z)$, and if $p(z)$ has degree n , we can go on to factorize $p(z)$ into n linear factors. The existence of such a factorization is of course another way to state the fundamental theorem.

Initially, interest was confined to polynomials $p(z)$ with real coefficients, and in this case d'Alembert (1746) observed that if $z = u + iv$ is a

solution of $p(z) = 0$, then so is its conjugate $\bar{z} = u - iv$. Thus the imaginary linear factors of a real $p(z)$ can always be combined in pairs to form real quadratic factors:

$$(z - u - iv)(z - u + iv) = z^2 - 2uz + (u^2 + v^2).$$

This gave another equivalent of the fundamental theorem: each (real) polynomial $p(z)$ can be expressed as a product of real linear and quadratic factors. The theorem was usually stated in this way during the 18th century, when its main purpose was to make possible the integration of rational functions (see previous section). This also avoided mention of $\sqrt{-1}$.

It has often been said that attempts to prove the fundamental theorem began with d'Alembert (1746), and that the first satisfactory proof was given by Gauss (1799). This opinion should not be accepted without question, since the source of it is Gauss himself. Gauss (1799) gave a critique of proofs from d'Alembert on, showing that they all had serious weaknesses, then offered a proof of his own. He wanted to convince readers that the new proof was the first valid one, even though it used one unproved assumption (which is discussed further in the next section). The opinion as to which of two incomplete proofs is more convincing can of course change with time, and I believe that Gauss (1799) might be judged differently today. We can now fill the gaps in d'Alembert (1746) by appeal to standard methods and theorems, whereas there is still no easy way to fill the gap in Gauss (1799). This was first done by Ostrowski (1920).

Both proofs depend on the geometric properties of the complex numbers and the concept of continuity for their completion. The basic geometrical insight—that the complex number $x + iy$ can be identified with the point (x, y) in the plane—mysteriously eluded all mathematicians until the end of the 18th century. This was one of the reasons that d'Alembert's proof was unclear, and the use of this insight by Argand (1806) was an important step in d'Alembert's reinstatement. Gauss seems to have had the same insight but concealed its role in his proof, perhaps believing that his contemporaries were not ready to view the complex numbers as a plane.

As for the concept of continuity, neither Gauss nor d'Alembert understood it very well. Gauss (1799) seriously understated the difficulties involved in the unproved step, claiming that “no one, to my knowledge, has ever doubted it. But if anybody desires it, then on another occasion I intend to give a demonstration which will leave no doubt” (translation from Struik (1969), p. 121). Perhaps seeing the difficulty on further reflec-

tion, he gave a second proof, Gauss (1816), in which the role of continuity was minimized. The second proof is purely algebraic except for the use of a special case of the intermediate value theorem. Gauss assumed that a polynomial function $p(x)$ of a real variable x takes all values between $p(a)$ and $p(b)$ as x runs from a to b (which implies that a polynomial of *odd* degree takes the value 0).

The first to appreciate the importance of continuity for the fundamental theorem of algebra was Bolzano (1817), who proved the continuity of polynomial functions and attempted a proof of the intermediate value theorem. The latter proof was unsatisfactory because Bolzano had no clear concept of real number on which to base it, but it did point in the right direction. When a definition of real numbers emerged in the 1870s (for example, with Dedekind cuts; Section 4.2), Weierstrass (1874) rigorously established the basic properties of continuous functions, such as the intermediate value theorem and extreme value theorem. This completed not only the second proof of Gauss but also the proof of d'Alembert, as we will see in the next subsection.

The Idea of d'Alembert

The key to d'Alembert's proof is a proposition now known as *d'Alembert's lemma*: if $p(z)$ is a nonconstant polynomial function and $p(z_0) \neq 0$, then any neighborhood of z_0 contains a point z_1 such that $|p(z_1)| < |p(z_0)|$.

The proof of this lemma offered by d'Alembert depended on solving the equation $w = p(z)$ for z as a fractional power series in w . As mentioned in Section 9.4, such a solution was claimed by Newton (1671), but it was made clear and rigorous only by Puiseux (1850). Thus d'Alembert's argument did not stand on solid ground, and in any case it was unnecessarily complicated.

A simple elementary proof of d'Alembert's lemma was given by Argand (1806). Argand was one of the co-discoverers of the geometric representation of complex numbers (probably the first was Wessel (1797), but his work remained almost unknown for 100 years), and he offered the following proof as an illustration of the effectiveness of the representation.

The value of $p(z_0) = x_0 + iy_0$ is interpreted as the point (x_0, y_0) in the plane, so that $|p(z_0)|$ is the distance of (x_0, y_0) from the origin. We wish to find a Δz such that $p(z_0 + \Delta z)$ is nearer to the origin than $p(z_0)$. If

$$p(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n,$$

then

$$\begin{aligned}
 p(z_0 + \Delta z) &= a_0(z_0 + \Delta z)^n + a_1(z_0 + \Delta z)^{n-1} + \cdots + a_n \\
 &= a_0 z_0^n + a_1 z_0^{n-1} + \cdots + a_n + A_1 \Delta z + A_2 (\Delta z)^2 + \cdots + A_n (\Delta z)^n \\
 &\quad \text{for some constants } A_i \text{ depending on } z_0, \text{ not all zero,} \\
 &\quad \text{because } p \text{ is not constant} \\
 &= p(z_0) + A \Delta z + \varepsilon,
 \end{aligned}$$

where $A = A_i(\Delta z)^i$ contains the first nonzero A_i and $|\varepsilon|$ is small compared with $|A \Delta z|$ when $|\Delta z|$ is small (because ε contains higher powers of Δz). It is then clear (Figure 11.3) that by choosing the direction of Δz so that $A \Delta z$ is opposite in direction to $p(z_0)$, we get $|p(z_0 + \Delta z)| < |p(z_0)|$. This completes the proof of d'Alembert's lemma.

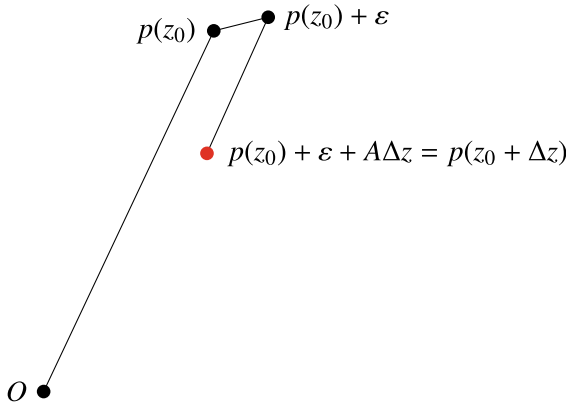


Figure 11.3: Construction for d'Alembert's lemma

To complete the proof of the fundamental theorem of algebra, take an arbitrary polynomial p and consider the continuous function $|p(z)|$. Since $p(z) \approx a_0 z^n$ for $|z|$ large, $|p(z)|$ increases with $|z|$ outside a sufficiently large circle $|z| = R$. We now get a z for which $|p(z)| = 0$ from the extreme value theorem of Weierstrass (1874); a continuous function on a closed bounded set assumes maximum and minimum values. By this theorem, $|p(z)|$ takes a minimum value for $|z| \leq R$. The minimum is ≥ 0 by definition, and if it is > 0 we get a contradiction by d'Alembert's lemma: either a point z with $|z| \leq R$ where $|p(z)|$ takes a value less than its minimum or a point z with $|z| > R$ where $|p(z)|$ is less than its values on $|z| = R$. Thus there is a point z where $|p(z)| = 0$ and hence $p(z) = 0$.

From our present perspective, d'Alembert's route to the fundamental theorem of algebra seems basically easy because it proceeds through general properties of continuous functions. The route of Gauss seems equally easy from a distance, but it goes through the still-unfamiliar territory of real algebraic curves. The intersections of real algebraic curves are harder to understand than the intersections of complex algebraic curves, and in retrospect they are harder to understand than the fundamental theorem of algebra. Indeed, as we will see in the next section, the fundamental theorem gives us Bézout's theorem, which in turn settles the problem of counting the intersections of complex algebraic curves.

EXERCISES

Complex roots of an equation with real coefficients occur in conjugate pairs because of the fundamental properties of conjugates.

11.4.1 Show directly from the definition $\overline{u + iv} = u - iv$ that

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2} \quad \text{and} \quad \overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$$

for any complex numbers z_1, z_2 .

11.4.2 Deduce from Exercise 11.4.1 that $p(\bar{z}) = \overline{p(z)}$ for any polynomial $p(z)$ with real coefficients, and hence that the complex roots of $p(z) = 0$ occur in conjugate pairs.

The expression in d'Alembert's lemma for $p(z_0 + \Delta z)$ is an instance of *Taylor's series*, previously discussed in Section 9.3. When the function is a polynomial p , as here, its Taylor series is finite because p has only finitely many nonzero derivatives.

11.4.3 Show that $A_1 = na_0z_0^{n-1} + (n-1)a_1z_0^{n-2} + \cdots + a_{n-1}$ and that the latter expression is $p'(z_0)$.

11.4.4 Show that $A_2 = \frac{n(n-1)}{2}a_0z_0^{n-2} + \frac{(n-1)(n-2)}{2}a_1z_0^{n-3} + \cdots + a_{n-2}$ and that the latter expression is $p''(z_0)/2$.

11.4.5 Using the binomial theorem, show that $A_k = p^{(k)}(z_0)/k!$, and hence that

$$p(z_0 + \Delta z) = a_0z_0^n + a_1z_0^{n-1} + \cdots + a_n + A_1\Delta z + A_2(\Delta z)^2 + \cdots + A_n(\Delta z)^n$$

is an instance of the Taylor series formula.

11.5 Roots and Intersections

There is a close connection between intersections of algebraic curves and roots of polynomial equations, going back as far as Menaechmus's construction of $\sqrt[3]{2}$ (a root of the equation $x^3 = 2$) by intersecting a parabola

and a hyperbola (Section 2.4). The most direct connection, of course, occurs in the case of a polynomial curve

$$y = p(x) \quad (1)$$

whose intersections with the axis $y = 0$ are just the real roots of the equation

$$p(x) = 0. \quad (2)$$

If (2) has k real roots, then the curve (1) has k intersections with the axis $y = 0$. Here we must count intersections the same way we count roots, according to *multiplicity*. A root r of (2) has multiplicity μ if the factor $(x - r)$ occurs μ times in $p(x)$, and the root r is then counted μ times.

This way of counting is also geometrically natural because if, for example, the curve $y = p(x)$ meets the axis $y = 0$ with multiplicity 2 at 0, then a line $y = \varepsilon x$ close to the axis meets the curve twice—once near the intersection with the axis and once precisely there. The intersection of $y = x^2$ with $y = 0$ (Figure 11.4) can therefore be considered as two *coincident points* to which the distinct intersections with $y = \varepsilon x$ tend as $\varepsilon \rightarrow 0$. Likewise, an intersection of multiplicity 3 can be explained as the limit of three distinct intersections, for example, of $y = \varepsilon x$ with $y = x^3$ (Figure 11.5)

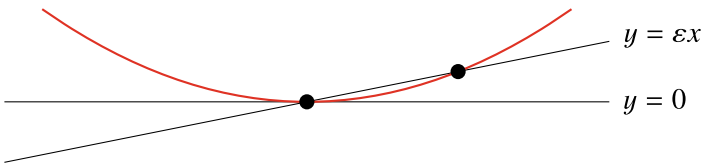


Figure 11.4: Intersection of multiplicity 2

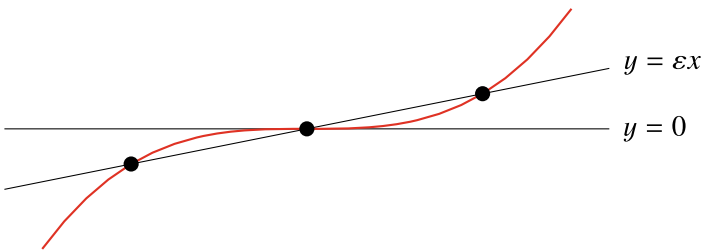


Figure 11.5: Intersection of multiplicity 3

At first glance this idea seems to break down with multiplicity 4, since $y = \varepsilon x$ meets $y = x^4$ at only two points, $x = 0$ and $x = \sqrt[3]{\varepsilon}$. The explanation is that there are also two complex roots in this case ($\sqrt[3]{\varepsilon}$ times the two complex cube roots of 1), hence we cannot neglect complex roots if we want to get the geometrically correct number of intersections.

The fundamental theorem of algebra (previous section) gives us n roots of an n th-degree equation (2) and hence n intersections of the polynomial curve (1) with the axis $y = 0$. To get n roots, however, we have to admit complex values of x , so we have to consider “curves” for which x and y are complex in order to obtain n intersections. This, and other tidy consequences of the fundamental theorem of algebra (for example, the “coincident point” interpretation of multiplicity; see Exercise 11.5.1), persuaded 18th-century mathematicians to admit complex numbers into the theory of curves before complex numbers themselves were understood—and even before the fundamental theorem of algebra was proved.

The most elegant consequence was Bézout’s theorem that a curve C_m of degree m meets a curve C_n of degree n at mn points. As we saw in Section 7.7, if homogeneous coordinates are used to take account of points at infinity, then the intersections of C_m and C_n correspond to the solutions of an equation $r_{mn}(x, y) = 0$, which is homogeneous of degree mn . We can now use the fundamental theorem of algebra to show that $r_{mn}(x, y)$ is the product of mn linear factors as follows:

$$\begin{aligned} r_{mn}(x, y) &= y^{mn} r_{mn}\left(\frac{x}{y}, 1\right) \\ &= y^{mn} \prod_{i=1}^p \left(b_i \frac{x}{y} - a_i\right) \quad \text{for some } p \leq mn \end{aligned}$$

by the fundamental theorem, since $r_{mn}(x/y, 1)$ is a polynomial of degree $p \leq mn$ in the single variable x/y . But then

$$\begin{aligned} r_{mn}(x, y) &= y^{mn-p} \prod_{i=1}^p (b_i x - a_i y) \\ &= \prod_{i=1}^{mn} (b_i x - a_i y) \end{aligned}$$

since each factor y in front (if any) is trivially of the form $b_i x - a_i y$.

It follows that the equation $r_{mn}(x, y) = 0$ has mn solutions, and hence there are mn intersections of C_m and C_n , counting multiplicities.

EXERCISES

11.5.1 Show that $y = \varepsilon x$ meets $y = x^n$ in n distinct points when $\varepsilon \neq 0$, and list them (for example, with the help of de Moivre's theorem).

If a curve K has a double point at O , then a line $y = tx$ may have double contact with K at O even though nearby lines $y = (t + \varepsilon)x$ do not meet K at nearby points other than O . In this case the double contact may be explained as contact with the two branches of the curve at O .

11.5.2 Consider the lines $y = tx$ through the double point O of $y^2 = x^2(x + 1)$. Show that each such line has double contact with the curve at O , except when $t = \pm 1$. How do you account for the multiplicities when $t = \pm 1$?

11.5.3 Show that $y = tx$ also has double contact with $y^2 = x^3$ at its cusp point O . Try to explain this by viewing $y^2 = x^3$ as the result of shrinking the loop of $y^2 = x^2(x + \varepsilon)$ (letting $\varepsilon \rightarrow 0$).

11.5.4 Show that the line $y = tx$ has double contact at O with the lemniscate $(x^2 + y^2)^2 = x^2 - y^2$ except for two values of t , for which it has quadruple contact.

11.5.5 Explain the multiplicities found in Exercise 11.5.4 with the help of the known shape of the lemniscate (Figure 10.4).

11.6 The Complex Projective Line

We saw in Section 7.5 that adding a point at infinity to the real line \mathbb{R} in $\mathbb{R} \times \mathbb{R}$ forms a closed curve that is qualitatively like a circle. Indeed, a real projective line in the sphere model of the real projective plane \mathbb{RP}^2 has much the same geometric properties as a great circle on a sphere, after one allows for the fact that antipodal points on the sphere are the same point on \mathbb{RP}^2 . The situation with the complex “line” \mathbb{C} is similar but more difficult to visualize. \mathbb{C} is already two-dimensional, as we saw in Gauss's proof of the fundamental theorem of algebra; hence the complex “plane” $\mathbb{C} \times \mathbb{C}$ is four-dimensional and virtually impossible to visualize.

To avoid an excursion into four-dimensional space, we first revise our approach to the real projective line. In Section 7.5 we considered ordinary lines L , in a horizontal plane not passing through the origin, and extended each to a projective line whose “points” are the lines through the origin O , in the plane through O and L . The nonhorizontal lines in this family correspond to points of L , and the horizontal line in the family to the point

at infinity of L . We now use this construction again to demonstrate directly the qualitative, or more precisely *topological*, equivalence between a projective line and a circle (Figure 11.6).

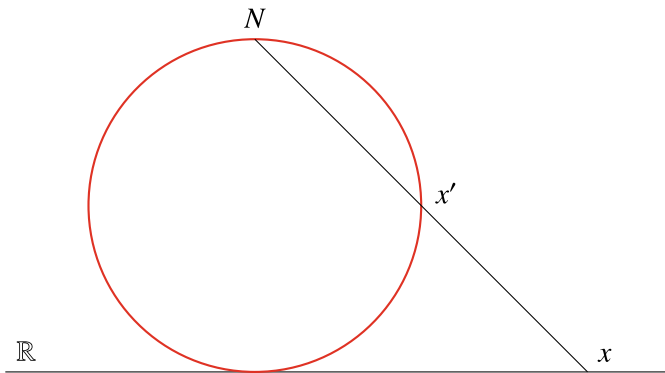


Figure 11.6: The real projective line

The origin N is taken to be the top point of a circle that, at its bottom point, touches our line $L = \mathbb{R}$. There is a continuous one-to-one correspondence between lines through N and points of the circle. Each nonhorizontal line corresponds to its intersection $x' \neq N$ with the circle, while the horizontal line corresponds to N itself. Thus the projective completion of \mathbb{R} , which we now call \mathbb{RP}^1 , is *topologically the same* as the circle, in the sense that there is a continuous one-to-one correspondence between them. Moreover, we can understand projective completion of \mathbb{R} topologically as a process of adding one “point” that is “approached” as one tends to infinity, in either direction, along \mathbb{R} , for as x tends to infinity in either direction, x' tends to the same point, N , on the circle.

We can now view projective completion of \mathbb{C} in the same way using Figure 11.7, which shows what is called *stereographic projection* of the plane \mathbb{C} into a sphere. Each point $z \in \mathbb{C}$ is projected to a point z' on the tangential sphere S by the ray through z and the north pole N of S . This establishes a continuous one-to-one correspondence between points z of \mathbb{C} and points $z' \neq N$ on S . Moreover, as z tends to infinity in any direction, z' tends to N ; hence the projective completion of \mathbb{CP}^1 of \mathbb{C} is topologically the same as the complete sphere S , with the point at ∞ of \mathbb{C} corresponding to N .

Since one also wants to complete \mathbb{C} by a point ∞ in this way for com-

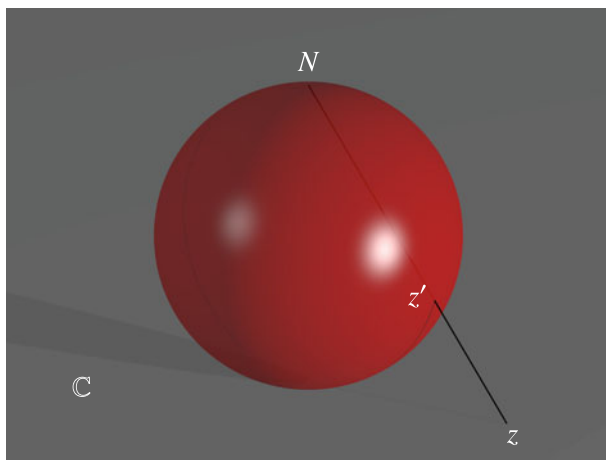


Figure 11.7: The complex projective line

plex analysis, geometry and analysis are both served by passing from \mathbb{C} to \mathbb{CP}^1 . Gauss seems to have been the first to appreciate the advantages of $\mathbb{C} \cup \{\infty\}$ over \mathbb{C} ; hence one often calls \mathbb{CP}^1 the *Gauss sphere* in analysis. (Unfortunately, only a few unpublished, undated fragments of Gauss’s work on this topic seem to have survived; see Gauss (1819).) Algebraic geometers call \mathbb{CP}^1 the (complex) projective line, since it is the formal equivalent of a real line, even though it is topologically a surface. Similarly, complex curves are topologically surfaces, known to analysts as *Riemann surfaces*, though algebraic geometers prefer to call them “curves.”

The “surface” viewpoint is helpful when studying intrinsic properties of complex curves. For example, *genus* (introduced in connection with parameterization in Sections 10.2 and 10.3) turns out to have a very simple meaning in the topology of surfaces (see Section 15.3). On the other hand, the “curve” viewpoint is helpful when studying intersections of curves and their embedding in $\mathbb{C} \times \mathbb{C}$ or its projective completion \mathbb{CP}^2 . Instead of trying to imagine two planes meeting in a single point of $\mathbb{C} \times \mathbb{C}$, for example, it is better to imagine the intersection as analogous to that of real lines in a real plane—as the single solution of two linear equations. After all, we are working with \mathbb{C} to remove anomalies that occur with \mathbb{R} , not for the sake of doing something different, and we expect that much of the behavior of real curves will recur with complex ones.

EXERCISES

Since addition and multiplication are continuous functions, it is quite easy to find one-to-one continuous maps between certain complex algebraic curves and the sphere.

- 11.6.1** Show that the projective completion of the curve $Y = X^2$ is topologically a sphere by considering its parameterization

$$X = t, \quad Y = t^2,$$

where t ranges over the sphere $\mathbb{C} \cup \{\infty\}$. Namely, show that the mapping $t \mapsto (t, t^2)$ is one-to-one and continuous.

- 11.6.2** Similarly show that the projective completion of $Y^2 = X^3$ is topologically a sphere by considering its parameterization

$$X = t^2, \quad Y = t^3$$

and the continuous mapping $t \mapsto (t^2, t^3)$.

- 11.6.3** Consider the mapping of the t sphere onto the projective completion of $Y^2 = X^2(X + 1)$ defined by $t \mapsto P(t)$, where $P(t)$ is the third intersection of the curve with the line $Y = tX$ through the double point (found in Exercise 6.4.2).

Show that this mapping is continuous and that it is one-to-one except at the points $t = \pm 1$, which are both mapped to the point O on the curve. Conclude that the curve is topologically the same as a sphere with two points identified (Figure 11.8).



Figure 11.8: A singular sphere

11.7 Branch Points

The key to the topological form of a complex curve $p(x, y) = 0$ lies in its *branch points*, the points α where the Newton–Puiseux expansion of y begins with a fractional power of $(x - \alpha)$ (see Section 9.4). The nature of branch points was first described by Riemann (1851) as part of a revolutionary new geometric theory of complex functions. Riemann’s idea, one of the most illuminating in the history of mathematics, was to represent a relation $p(x, y) = 0$ between complex x and complex y by covering a plane (or sphere) representing the x variable by a surface representing the y variable, the point or points of the y surface over a given point $x = \alpha$ being those values of y that satisfy $p(\alpha, y) = 0$.

If the equation $p(\alpha, y) = 0$ is of degree n in y , there will in general be n distinct y values for a given α , consequently n *sheets* of the y surface lying over the x -plane in the neighborhood of $x = \alpha$. At finitely many exceptional values of x , sheets merge due to coincidence of roots, and the Newton–Puiseux theory says that at such a point y behaves like a fractional power of x at 0. Our main problem, therefore, is to understand the behavior of the Riemann surface for $y = x^{m/n}$ in the neighborhood of 0.

The idea can be grasped sufficiently well from seeing the special case $y = x^{1/2}$. If we consider the unit disk in the y -plane and try to deform it so that the points $y = \pm \sqrt{x}$ lie above the point x in the unit disk of the x -plane, then the result is something like Figure 11.9.

The angles θ on the disk boundaries are the arguments of the corresponding points $e^{i\theta} = \cos \theta + i \sin \theta$, as we explain in Section 12.1. If

$$x = e^{i\theta} = e^{i(\theta+2\pi)}$$

then

$$y = e^{i\theta/2}, \quad e^{i(\theta/2+\pi)},$$

giving the values shown.

It should be noted that the awkward appearance of the branch point, in particular the line of self-intersection, is a consequence of representing the relation $y^2 = x$ in fewer dimensions than the four it really requires. If we similarly attempt to represent the relation $y^2 = x$ between real x and y by laying the y -axis along the x -axis so that $y = \pm \sqrt{x}$ are on top of x , then the result is an awkward folded “branch point” at 0 (Figure 11.10). This is a consequence of trying to represent the relation in one dimension. In reality,

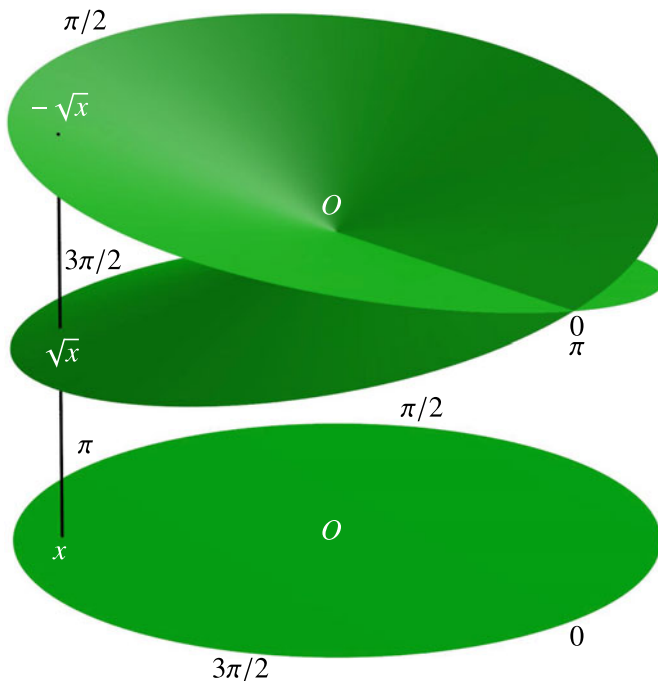


Figure 11.9: Branch point for the square root

as the second part of the figure shows, when viewed as a curve in the plane the relation is just as smooth at 0 as anywhere else. (Notice, incidentally, that the folded line in Figure 11.10, the real y -axis, corresponds to the self-intersection line in Figure 11.9.)

11.8 Topology of Complex Projective Curves

To understand the complete structure of the complex projective curve defined by $y^2 = x$ we need to know its behavior at infinity. At ∞ there is another branch point like the one at 0 (just replace x by $1/u$ and y by $1/v$ and notice that we are looking at $v^2 = u$ near $y = 0$, $v = 0$ —the same situation as before). The topological nature of the relation between x and y can then be captured by the model seen in Figure 11.11. The sphere of x values is covered by two spheres (like skins of an onion), slit along a line from 0 to ∞ and cross-joined by pasting the red edges together and the purple

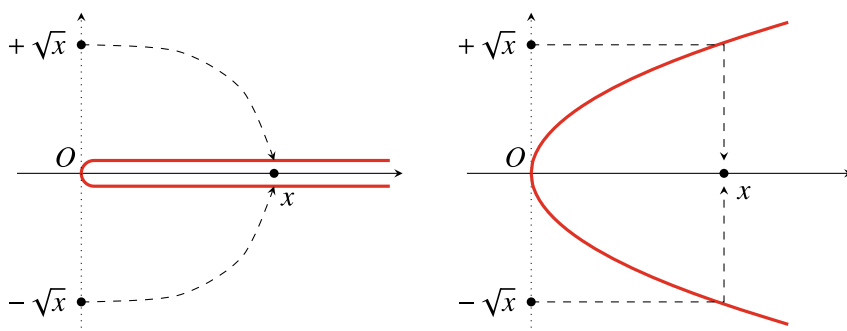


Figure 11.10: Branch point in one dimension and two

edges together. The slit from 0 to ∞ is arbitrary, but the cross-joining is needed to produce the branch point structure at 0 and ∞ .

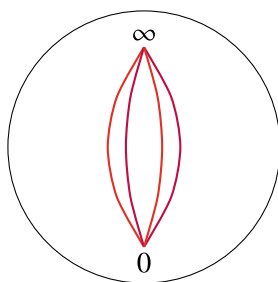


Figure 11.11: Covering the sphere

The covering of the x sphere by this two-sheeted surface expresses the *covering projection map* $(x, y) \mapsto x$ from a general point on the curve $y^2 = x$ to its x coordinate and shows that it is two-to-one except at the branch points 0, ∞ . The two-sheeted surface itself captures the intrinsic topological structure of the curve, and this structure can be more readily seen by separating the two skins from the x sphere and each other, then joining the required edges (Figure 11.12). Edges to be joined are given the same color, and we see that the resulting surface is topologically a sphere.

This result could have been obtained more directly by projecting each point (x, y) on the curve to y , since this is a one-to-one continuous map between the curve and the y -axis, which we know to be topologically a sphere (when ∞ is included). The curve here was modeled by cutting and joining sheets on the sphere because this method extends to all algebraic

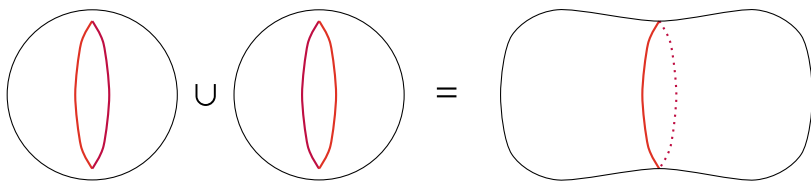


Figure 11.12: Joining the separated sheets

curves. The Newton–Puiseux theory implies that any algebraic relation $p(x, y) = 0$ can be modeled by a finite-sheeted covering of the sphere, with finitely many branch points. The most general branch point structure is given by a prescription for cross-joining (permuting) the sheets, and by slitting the sheets between branch points (or, if necessary, to an auxiliary point) they can be rejoined to produce the prescribed branching behavior.

The most interesting case of this method is the cubic curve

$$y^2 = x(x - \alpha)(x - \beta).$$

This relation defines a covering in the x sphere that is two-sheeted, since for each x there are $+$ and $-$ values for y , with branch points at 0 , α , β , and ∞ . (The branch point at ∞ is explained in the exercises below.) Thus if we slit the sheets from 0 to α and from β to ∞ , the required joining is by pasting like-colored edges, as shown in Figure 11.13.

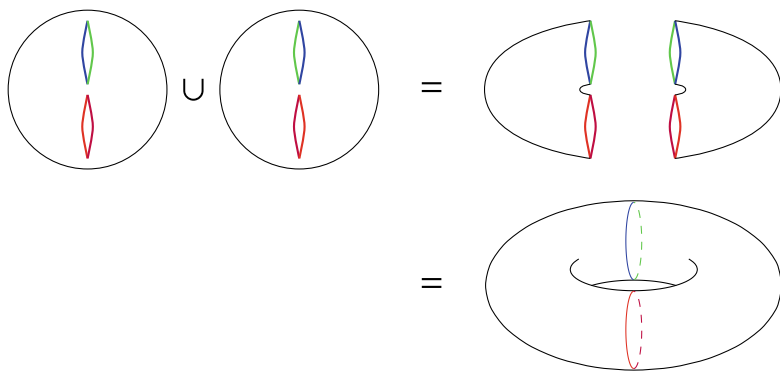


Figure 11.13: Joining the sheets of a cubic curve

We find, as Riemann did, that the surface is a torus, and hence *not* topologically the same as a sphere. This discovery illuminated the theory of cubic curves and elliptic functions, as we will see in the next chapter.

One quickly sees that relations of the form

$$y^2 = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{2n})$$

yield Riemann surfaces of all the forms shown in Figure 11.14. These surfaces are distinguished topologically from each other by the number of “holes”: 0 for the sphere, 1 for the torus, and so on. This simple topological invariant turns out to be the *genus*, which also determines the type of functions that can parameterize the corresponding complex curve. Other geometric and analytic properties of genus will unfold over the next few chapters. The topological importance of genus was established by Möbius (1863), when he showed that any closed surface in ordinary space is topologically equivalent to a sphere or one of the forms seen in Figure 11.14. For more on genus, see Chapter 15.



Figure 11.14: Riemann surfaces of genus 1, 2, 3, ...

EXERCISES

We can transfer the “one-dimensional branch point” (Figure 11.10) to infinity to see the topology of the real projective curve $y^2 = x$.

- 11.8.1** Explain why the real projective curve $y^2 = x$ has a branch point at infinity like the one at 0, and hence conclude that this curve is topologically a circle.

We can explain the branch point at infinity of a cubic curve as follows.

- 11.8.2** Use the substitution $x = 1/u$, $y = 1/v$ to show that the curve

$$y^2 = x(x - \alpha)(x - \beta)$$

behaves at infinity as the curve

$$v^2 = u^3(1 - u\alpha)^{-1}(1 - u\beta)^{-1}$$

does at 0, which in turn is qualitatively like the behavior of

$$v = u^{3/2}.$$

- 11.8.3** Show, by considering the points lying above $u = e^{i\theta}$, that $v = u^{3/2}$ has a branch point at 0 like that of $v = u^{1/2}$.



12

Complex Numbers and Functions

PREVIEW

The insight into algebraic curves afforded by complex coordinates—that a complex curve is topologically a surface—has important implications for functions defined as integrals of algebraic functions, such as the logarithm, exponential, and elliptic functions.

The complex logarithm turns out to be many-valued, due to the different paths of integration in the complex plane between the same endpoints. It follows that its inverse function, the exponential function, is *periodic*. In fact, the complex exponential function is a fusion of the real exponential function with the sine and cosine: $e^{x+iy} = e^x(\cos y + i \sin y)$.

The double periodicity of elliptic functions also becomes clear from the complex viewpoint. The integrals that define them are taken over paths on a *torus* surface, on which there are two independent closed paths.

The two-dimensional nature of complex numbers imposes interesting and useful constraints on the nature of *differentiable* complex functions. Such functions define *conformal* (angle-preserving) maps between surfaces. Also, their real and imaginary parts satisfy equations, called the *Cauchy–Riemann* equations, that govern fluid flow. So complex functions can be used to study the motion of fluids.

Finally, the Cauchy–Riemann equations imply *Cauchy’s theorem*. This fundamental theorem guarantees that differentiable complex functions have many good features, such as power series expansions.

12.1 Complex Functions

When Bombelli (1572) introduced complex numbers, he implicitly introduced complex functions as well. The solution y of the cubic equation $y^3 = py + q$,

$$y = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}} + \sqrt[3]{\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}},$$

involves the cube root of a complex argument when $(q/2)^2 < (p/3)^3$. It could have been a revelation to see that complex numbers explain the coincidence of algebraic (Cardano) and geometric (Viète) solutions of the cubic equation, and more generally the Leibniz–de Moivre theorem that

$$x = \frac{1}{2} \sqrt[n]{y + \sqrt{y^2 - 1}} + \frac{1}{2} \sqrt[n]{y - \sqrt{y^2 - 1}},$$

when $x = \sin \theta$ and $y = \sin n\theta$ (Section 5.6). In the case of the cubic, this revelation can now be savored in Needham (1997), pp. 59–60. But mathematicians were not concerned about the meaning of these complex functions as long as they produced results that could be checked by algebra.

The need to *understand* complex functions became pressing only with transcendental functions, particularly those defined by integration. A key example is the logarithm function, which comes from integrating $dz/(1+z)$. Once this function was understood, the reason for algebraic miracles like the Leibniz–de Moivre theorem became much clearer.

Johann Bernoulli (1702) opened the story of the complex logarithm when he noted that

$$\frac{dz}{1+z^2} = \frac{dz}{2(1+z\sqrt{-1})} + \frac{dz}{2(1-z\sqrt{-1})}$$

and drew the conclusion that “imaginary logarithms express real circular sectors.” He did not actually perform the integration, but he may have found

$$\tan^{-1} z = \frac{1}{2i} \log \frac{i-z}{i+z},$$

since Euler gives him credit for a similar formula when writing to him in Euler (1728b). However, this may have been the young Euler’s defer-

ence to his former teacher, because Johann Bernoulli showed poor understanding of logarithms as the correspondence continued. He persistently claimed that $\log(-x) = \log(x)$ on the grounds that

$$\frac{d}{dx} \log(-x) = \frac{1}{x} = \frac{d}{dx} \log(x)$$

despite a reminder from Euler (1728b) that equality of derivatives does not imply equality of integrals. Euler went on to suggest that the complex logarithm had infinitely many values.

In the meantime, Cotes (1714) had also discovered a relation between complex logarithms and circular functions:

$$\log(\cos x + i \sin x) = ix.$$

Recognizing the importance of this result, he entitled his work *Harmonia mensurarum* (Harmony of measures). The “measures” in question were the logarithm and inverse tangent functions, which measure the hyperbola and the circle, respectively, via the integrals $\int dx/(1+x)$ and $\int dx/(1+x^2)$. A wide class of integrals had been reduced to these two types, but it was not understood why two apparently unrelated “measures” should be required. Cotes’s result was the first (apart from the near-miss of Johann Bernoulli) to relate the two, showing that in the wider domain of complex functions the logarithm and inverse circular functions are essentially the same.

The most compact statement of their relationship was reached around 1740, when Euler shifted attention from the logarithm function to its inverse, the exponential function. The definitive formula

$$e^{ix} = \cos x + i \sin x$$

was first published by Euler (1748a), who derived it by comparing series expansions of both sides. Euler’s formulation in terms of the single-valued function e^{ix} gave a simple explanation of the many values of the logarithm (which Cotes had missed) as a consequence of the periodicity of \cos and \sin . A direct explanation, based on the definition of \log as an integral, became possible when Gauss (1811) clarified the meaning of complex integrals and pointed out their dependence on the path of integration (see Section 12.3).

Euler’s formula also shows that

$$(\cos x + i \sin x)^n = e^{inx} = \cos nx + i \sin nx$$

and hence gives a deeper explanation of the Leibniz–de Moivre formula. More generally, the addition theorems for \cos and \sin (Section 10.6) could be seen as consequences of the much simpler addition formula for the exponential function

$$e^{u+v} = e^u \cdot e^v.$$

The imaginary function e^{ix} was so much more coherent than its real constituents $\cos x$ and $\sin x$ that it was difficult to do without it, and Euler’s formula gave mathematicians a strong push toward the eventual acceptance of complex numbers. A more detailed account of the role of the logarithm and exponential functions in the development of complex numbers may be found in Cajori (1913).

The Cauchy-Riemann Equations

At almost the same time that Euler elucidated cosine and sine, d’Alembert found many real functions occurring naturally in pairs as the real and imaginary parts of complex functions. In hydrodynamics, d’Alembert (1752) discovered that the equations

$$\frac{\partial P}{\partial y} - \frac{\partial Q}{\partial x} = 0 \quad \text{and} \quad \frac{\partial P}{\partial x} + \frac{\partial Q}{\partial y} = 0$$

relate the velocity components P , Q in two-dimensional steady irrotational fluid flow. These equations come from the requirements that $Q dx + P dy$ and $P dx - Q dy$ be complete differentials, in which case another complete differential is

$$Q dx + P dy + i(P dx - Q dy) = (Q + iP) \left(dx + \frac{dy}{i} \right) = (Q + iP) d \left(x + \frac{y}{i} \right).$$

D’Alembert concluded that this means $Q + iP$ is a function f of $x + y/i$, so that $Q = \operatorname{Re}(f)$ and $P = \operatorname{Im}(f)$.

To feel the force of this result, one has to forget the modern definition of function, under which $u(x, y) + iv(x, y)$ is a function of $x + iy$ for any functions u, v . In the 18th-century context, a “function” $f(x + iy)$ of $x + iy$ was calculable from $x + iy$ by elementary operations; at worst, $f(x + iy)$ was a power series in $x + iy$. This imposes a strong constraint on u, v , namely that

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \quad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}.$$

These were just the equations d'Alembert found in his hydrodynamical investigations, but they came to be named the Cauchy–Riemann equations, because Cauchy and Riemann stressed their key role in the study of complex functions. The concept of complex function was solidified when Cauchy (1837) showed that a function $f(z)$, where $z = x + iy$, merely had to be differentiable in order to be expressible as a power series in z . Thus it suffices to define a complex function $f(z)$ as one that is differentiable with respect to z in order to guarantee that f is defined with 18th-century strictness. It follows, in particular, that the first derivative of f entails derivatives of all orders and that the values of f in any neighborhood determine its values everywhere. This rigidity in the notion of complex function is enough of a constraint to enable nontrivial properties to be proved, but at the same time it leaves enough flexibility—one might say “fluidity”—to cover important general situations.

EXERCISES

Euler's derivation of $e^{ix} = \cos x + i \sin x$ is easy to explain using the power series

$$e^y = 1 + \frac{y}{1!} + \frac{y^2}{2!} + \frac{y^3}{3!} + \cdots$$

and

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots$$

found in Section 8.5.

12.1.1 Assuming that the series for e^y is also valid for $y = ix$, show that

$$e^{ix} = \left(1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots\right) + i\left(x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots\right).$$

12.1.2 Assuming it is valid to differentiate the sine series term by term, show that

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots,$$

and hence that $e^{ix} = \cos x + i \sin x$.

Another consequence of $e^{ix} = \cos x + i \sin x$ is that $i = \cos \frac{\pi}{2} + i \sin \frac{\pi}{2} = e^{i\pi/2}$, which allows us to evaluate the outlandish number i^i .

12.1.3 Show that i^i has a real value (Euler (1746)). What is it?

12.1.4 Using the fact that $e^{2in\pi} = 1$ for any integer n , give a formula for all values of i^i (Euler (1746)).

12.2 Conformal Mapping

Another important general situation clarified by complex functions is the problem of conformal mapping. Mapping a sphere (the earth's surface) onto a plane is a practical problem that has attracted the attention of mathematicians since ancient times. Before the 18th century, the most notable mathematical contributions to mapping were stereographic projection (Section 11.6), due to Ptolemy around 150 CE, and the Mercator projection used by G. Mercator in 1569 (this Mercator was Gerard, not the Nicholas who discovered the series for $\log(1+x)$). Both these projections were conformal, that is, angle-preserving, or what 18th-century mathematicians called “similar in the small.” This means that the image $f(R)$ of any region R tends toward an exact scale map of R as the size of R tends to 0. Since “similarity in the large” is clearly impossible—for example, a great circle cannot be mapped to a closed curve that divides the plane into two equal parts—conformality is the best one can do to preserve the appearance of regions on the sphere. Preservation of angles was intentional in the Mercator projection, whose purpose was to assist navigation, and in the case of stereographic projection conformality was first noticed by Harriot around 1590 (see Lohne (1979)).

Figure 12.1 illustrates the conformality of stereographic projection in the case of spherical triangles. The sphere has been divided into triangles with angles $\pi/2, \pi/3, \pi/4$, and every other triangle has been cut out to allow a light to shine from inside the sphere and to cast shadows on the plane. It can be seen that the shadow triangles indeed have the same angles as their counterparts on the sphere. (This example shows another feature of stereographic projection: it maps circles to circles.)

Advances in the theory of conformal mapping were made by Lambert (1772), Euler (1777) (sphere onto plane), and Lagrange (1779) (general surface of revolution onto plane). All these authors used complex numbers, but Lagrange's presentation is the clearest and most general. Using the method of d'Alembert (1752), he combined a pair of differential equations in two real variables into a single equation in one complex variable and arrived at the result that any two conformal maps of a surface of revolution onto the (x, y) -plane are related via a complex function $f(x + iy)$ mapping the plane onto itself. These results were crowned by the result of Gauss (1822) generalizing Lagrange's theorem to conformal maps of an arbitrary surface onto the plane.



Figure 12.1: Example of stereographic projection

Conversely, a complex function $f(z)$ defines a map of the z plane into itself, and it is easy to see that this map is conformal. In fact, this is a consequence of the differentiability of f . To say that a nonzero limit

$$\lim_{\delta z \rightarrow 0} \frac{f(z_0 + \delta z) - f(z_0)}{\delta z}$$

exists is to say that the mapping of the disk $\{z : |z - z_0| < |\delta z|\}$ around z_0 to the region around $f(z_0)$ tends to a scale mapping as $|\delta z|$ tends to 0. If the derivative is expressed in polar form as

$$f'(z_0) = re^{i\alpha},$$

then r is the scale factor of this limit mapping and α is the angle of rotation. Riemann (1851) seems to have been the first to take the conformal mapping property as a basis for the theory of complex functions. His deepest result in this direction was the *Riemann mapping theorem*, which states that any region of the plane bounded by a simple closed curve can be mapped onto the unit disk conformally, and hence by a complex function. The proof of this theorem in Riemann (1851) depends on properties that Riemann justified partly by an appeal to physical intuition that he called *Dirichlet's principle*. Such reasoning went against the growing tendency toward rigor in 19th-century analysis, and stricter proofs were given by Schwarz (1870) and Neumann (1870). However, Riemann's faith in the physical roots of complex function theory was eventually justified when Hilbert (1900b) put Dirichlet's principle on a sound basis.

EXERCISES

The claim that differentiability of $f(z)$ implies that f is a conformal mapping must be qualified by the condition $f'(z) \neq 0$, because if the scale factor tends to 0 then f cannot be said to be a scale mapping. At points where $f'(z) = 0$ one may find that angles are altered. Here is an example.

12.2.1 Show that $f(z) = z^2$ defines a conformal mapping except at $z = 0$, where it doubles angles.

This is no surprise because $z \mapsto z^2$ is a two-sheeted covering of the plane \mathbb{C} (see Figure 11.9 in Section 11.7).

12.2.2 Show that the map $z \mapsto z^2$ is two-to-one except at $z = 0$, and relate the angle doubling at $z = 0$ to the branch point of the covering.

12.2.3 Similarly describe the behavior of the map $z \mapsto z^3$ at $z = 0$.

12.3 Cauchy's Theorem

We have seen that interesting complex functions arise from integration. For example, the elliptic functions come from inversion of elliptic integrals (Section 10.8). However, it is not at first clear what the integral $\int_{z_0}^z f(t) dt$ means when z_0, z are complex numbers. It is natural, and not technically difficult, to define $\int_{z_0}^z f(t) dt$ as $\int_C f(t) dt$, the integral of f along a curve C from z_0 to z ; the problem is that $\int_C f(t) dt$ appears to depend on C and hence may not be a function of z .

The first to recognize and resolve this problem seems to have been Gauss. In a letter to Bessel, Gauss (1811) raised the problem and claimed its resolution as follows:

Now how is one to think of $\int \Phi(z) dz$ for $z = a + ib$? Evidently, if one wishes to start from clear concepts, one must assume that z changes by infinitely small increments (each of the form $\alpha + i\beta$) from that value for which the integral is to be 0 to $c = a + ib$, and then *sum* all the $\phi(z) dz \dots$ But now \dots continuous transition from one value of z to another $a + ib$ takes place along a curve and hence is possible in infinitely many ways. I now conjecture that the integral $\int_0^c \phi(z) dz$ will always have the same value after two different transitions if $\phi(z)$ never becomes infinite within the region enclosed by the two curves representing the transitions.

Translation of Gauss (1811) in Birkhoff (1973), p. 31

In the same letter, Gauss also observed that if $\phi(z)$ *does* become infinite in the region, then in general $\int_0^c \phi(z) dz$ *will* take different values when integrated along different curves. He saw in particular that the infinitely many values of $\log c$ corresponded to the different ways a path from 1 to c could wind around $z = 0$, the point where $\phi(z) = 1/z$ becomes infinite.

The theorem that $\int_{z_0}^z f(t) dt$ is independent of the path in a region where f is finite (and differentiable, which went without saying for Gauss) is now known as *Cauchy's theorem*, since Cauchy was the first to offer a proof and to develop the consequences of the theorem. An equivalent statement is that $\int_C f(t) dt = 0$ for any closed curve C in a region where f is differentiable. Cauchy presented a proof to the Paris Academy in 1814 but first published it later (Cauchy (1825)). In Cauchy (1846) he gave a more transparent proof, based on the Cauchy–Riemann equations and the theorem of Green (1828) and Ostrogradsky (1828), relating a line integral to a surface integral. The latter theorem, usually known as *Green's theorem*, is a generalization of the fundamental theorem of calculus to real functions $g(x, y)$ of two variables and can be stated as follows: if C is a simple closed curve bounding a region \mathcal{R} and g is suitably smooth, then

$$\int_C g dx = \iint_{\mathcal{R}} \frac{\partial g}{\partial y} dx dy, \quad \text{and} \quad \int_C g dy = - \iint_{\mathcal{R}} \frac{\partial g}{\partial x} dx dy,$$

where $\iint_{\mathcal{R}}$ is the surface integral over \mathcal{R} and \int_C is the line integral around C in the counterclockwise sense. (The difference in sign in the two formulas reflects the different sense of C when x and y are interchanged.)

Cauchy's theorem follows from Green's by an easy calculation. If

$$f(t) = u(t) + iv(t)$$

is the decomposition of f into real and imaginary parts, and if we write

$$dt = dx + i dy,$$

then

$$\begin{aligned} \int_C f(t) dt &= \int_C (u + iv)(dx + i dy) \\ &= \int_C (u dx - v dy) + i \int_C (v dx + u dy) \\ &= \iint_{\mathcal{R}} \left(\frac{\partial u}{\partial y} + \frac{\partial v}{\partial x} \right) dx dy + i \iint_{\mathcal{R}} \left(\frac{\partial v}{\partial y} - \frac{\partial u}{\partial x} \right) dx dy, \end{aligned}$$

which equals 0 since

$$\frac{\partial u}{\partial y} + \frac{\partial v}{\partial x} = 0 \quad \text{and} \quad \frac{\partial v}{\partial y} - \frac{\partial u}{\partial x} = 0$$

by the Cauchy–Riemann equations. This proof requires f to have a continuous first derivative in order to be able to apply Green’s theorem. The restriction of continuity of $f'(t)$ in the proof was removed by Goursat (1900). As it happens, if f' exists, it will have not only continuity but also derivatives of all orders.

This follows from one of the remarkable consequences Cauchy (1837) drew from the assumption $\int_C f(t) dt = 0$, namely, that f has a power-series expansion. By Goursat (1900), then, differentiability of a complex function is enough to guarantee a power-series expansion. A generalization of this result to f that become infinite at isolated points was made by Laurent (1843) (f then has an expansion including negative powers, called the *Laurent expansion*) and to many-valued f with branch points by Puiseux (1850) (f then has an expansion in fractional powers, the *Newton–Puiseux expansion*).

EXERCISES

The Cauchy–Riemann equations follow easily from the existence of $f'(z)$, that is, from the condition that

$$\lim_{\delta z \rightarrow 0} \frac{f(z + \delta z) - f(z)}{\delta z}$$

have the same value, regardless of the path along which $\delta z \rightarrow 0$.

- 12.3.1** Suppose $f(z) = u(x, y) + iv(x, y)$ and $\delta z = \delta x + i\delta y$. By letting $\delta z \rightarrow 0$ along the x -axis ($\delta y = 0$) and along the y -axis ($\delta x = 0$), and equating the resulting values of $f'(z)$, show that

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \quad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}.$$

These equations give a convenient test for a function $u(x, y) + iv(x, y)$ to be a differentiable function of $z = x + iy$.

- 12.3.2** Check that $u(x, y) = x^2 - y^2$ and $v(x, y) = 2xy$ satisfy the Cauchy–Riemann equations.

- 12.3.3** Express $x^2 - y^2 + 2ixy$ as a function of $z = x + iy$.

12.4 Double Periodicity of Elliptic Functions

The view of complex integration exposed by Cauchy's theorem is one step toward understanding elliptic integrals such as $\int_0^z dt / \sqrt{t(t-\alpha)(t-\beta)}$. The other important step is the idea of a Riemann surface (Section 11.8), which enables us to visualize the possible paths of integration from 0 to z . The "function" $1/\sqrt{t(t-\alpha)(t-\beta)}$ is of course two-valued and, by an argument like that in Section 11.8, is represented by a two-sheeted covering of the t sphere, with branch points at 0, α , β , ∞ . Thus the paths of integration, correctly viewed, are curves on this surface, which is topologically a torus (again, as in Section 11.8).

Now a torus contains certain closed curves that do not bound a piece of the surface, such as the red and blue curves, C_1 and C_2 , shown in Figure 12.2. There is no region \mathcal{R} bounded by C_1 or C_2 ; hence Green's theorem does not apply, and we in fact obtain nonzero values

$$\begin{aligned}\omega_1 &= \int_{C_1} \frac{dt}{\sqrt{t(t-\alpha)(t-\beta)}}, \\ \omega_2 &= \int_{C_2} \frac{dt}{\sqrt{t(t-\alpha)(t-\beta)}}.\end{aligned}$$

Consequently the integral

$$\Phi^{-1}(z) = \int_0^z \frac{dt}{\sqrt{t(t-\alpha)(t-\beta)}}$$

will be ambiguous: for each value $\Phi^{-1}(z) = w$ obtained for a certain path C from 0 to z we also obtain the values $w + m\omega_1 + n\omega_2$ by adding to C a detour that winds m times around C_1 and n times around C_2 . (For topological reasons, this is essentially the most general path of integration.)

It follows that the inverse relation $\Phi(w) = z$, the elliptic function corresponding to the integral, satisfies

$$\Phi(w) = \Phi(w + m\omega_1 + n\omega_2)$$

for any integers m, n . That is, Φ is doubly periodic, with periods ω_1, ω_2 . This intuitive explanation of double periodicity is due to Riemann (1851), who later (Riemann (1858a)) developed the theory of elliptic functions from this standpoint.

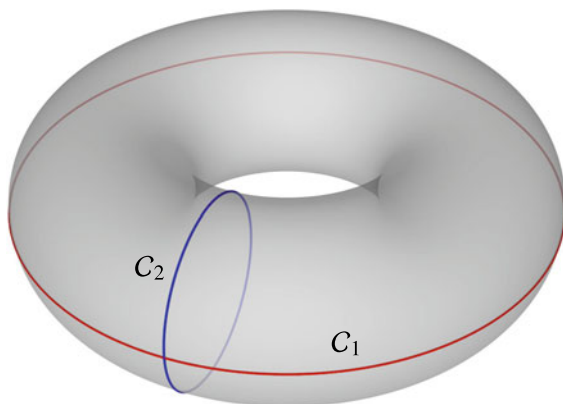


Figure 12.2: Nonbounding curves on the torus

Remarkable series expansions of elliptic functions, which exhibit the double periodicity analytically, were discovered by Eisenstein (1847). The precedents for Eisenstein's series, as Eisenstein himself pointed out, were partial fraction expansions of circular functions discovered by Euler, for example

$$\pi \cot \pi x = \sum_{n=-\infty}^{\infty} \frac{1}{x+n}$$

(Euler (1748a), p. 191). It is obvious (at least formally, though one has to be a little careful about the meaning of this summation to ensure convergence) that the sum is unchanged when x is replaced by $x+1$; hence the period 1 of $\pi \cot \pi x$ is exhibited directly by its series expansion. Eisenstein showed that doubly periodic functions could be obtained by analogous expressions, such as

$$\sum_{m,n=-\infty}^{\infty} \frac{1}{(z+m\omega_1+n\omega_2)^2},$$

which again (with suitable interpretation to ensure convergence) are obviously unchanged when z is replaced by $z+\omega_1$ or $z+\omega_2$. Hence we obtain a function with periods ω_1, ω_2 . The function above is in fact identical (up to a constant) with the Weierstrass \wp -function, mentioned in Section 10.7 as the inverse to the integral $\int dt/\sqrt{4t^3-g_2t-g_3}$. Weierstrass (1863), p. 121,

found the relations between g_2, g_3 and the periods ω_1, ω_2 :

$$g_2 = 60 \sum \frac{1}{(m\omega_1 + n\omega_2)^4},$$

$$g_3 = 140 \sum \frac{1}{(m\omega_1 + n\omega_2)^6},$$

where the sums are over all pairs $(m, n) \neq (0, 0)$. Elegant modern accounts of the Eisenstein and Weierstrass theories may be found in Weil (1976) and Robert (1973).

EXERCISES

The precise definition of the Weierstrass \wp -function is

$$\wp(z) = \frac{1}{z^2} + \sum_{m,n \neq 0,0}^{\infty} \left(\frac{1}{(z + m\omega_1 + n\omega_2)^2} - \frac{1}{(m\omega_1 + n\omega_2)^2} \right).$$

This series has better convergence than the Eisenstein series given above, but its double periodicity is not quite so obvious. We can establish double periodicity by differentiating and integrating as follows (which is valid because of the convergence properties of the Weierstrass series).

12.4.1 By differentiating term by term, show that

$$\wp'(z) = -2 \sum_{m,n=-\infty}^{\infty} \frac{1}{(z + m\omega_1 + n\omega_2)^3},$$

and conclude that $\wp'(z + \omega_1) = \wp'(z)$ and $\wp'(z + \omega_2) = \wp'(z)$.

12.4.2 By integrating the equations just obtained, show that

$$\wp(z + \omega_1) - \wp(z) = c \quad \text{and} \quad \wp(z + \omega_2) - \wp(z) = d,$$

for some constants c and d .

12.4.3 Deduce from Exercise 12.4.2 that

$$\wp\left(\frac{\omega_1}{2}\right) - \wp\left(-\frac{\omega_1}{2}\right) = c \quad \text{and} \quad \wp\left(\frac{\omega_2}{2}\right) - \wp\left(-\frac{\omega_2}{2}\right) = d.$$

12.4.4 But $\wp(z) = \wp(-z)$ (why?); hence conclude that \wp is doubly periodic.

12.5 Elliptic Curves

We have seen that nonsingular cubic curves of the form

$$y^2 = ax^3 + bx^2 + cx + d \quad (1)$$

are important not only among the cubic curves themselves (see Newton's classification, Sections 6.4 and 7.4), but also in number theory (Section 10.3) and the theory of elliptic functions (Section 10.4). One of the great achievements of 19th-century mathematics was finding a unified view of all these aspects of cubic curves. The view was glimpsed by Jacobi (1834), and it came more clearly into focus with the development of complex analysis between Riemann (1851) and Poincaré (1901). The theory of elliptic curves, as the unified view is now known, continues to inspire researchers today, since it seems to encompass some of the most fascinating problems of number theory. We now know, for example, how to derive Fermat's last theorem (see Section 10.1) from properties of elliptic curves.

Jacobi saw, at least implicitly, that the curve (1) could be parameterized as

$$x = f(z), \quad y = f'(z), \quad (2)$$

where f and its derivative f' are elliptic functions. Knowing that f and f' are doubly periodic, with the same periods ω_1, ω_2 , say, he would have seen that this gave a map of the z plane \mathbb{C} onto the curve (1) for which the preimage of a given point on (1) is a set of points in \mathbb{C} of the form

$$z + \Lambda = \{z + m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\},$$

where

$$\Lambda = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}.$$

Λ is called the *lattice of periods* of f . The numbers $z + m\omega_1 + n\omega_2$ in $z + \Lambda$ are said to be equivalent with respect to Λ . One such equivalence class is shown by asterisks inside parallelograms in Figure 12.3.

The parameterization (2) gives a one-to-one correspondence between the points $(f(z), f'(z))$ of the curve and the equivalence classes $z + \Lambda$. Today we say that the curve is *isomorphic to the space* \mathbb{C}/Λ of these equivalence classes. Jacobi might have seen, though it was probably not of interest to him, that \mathbb{C}/Λ is a torus. One sees this by taking one parallelogram in \mathbb{C} , which includes a representative of each equivalence class, and identifying

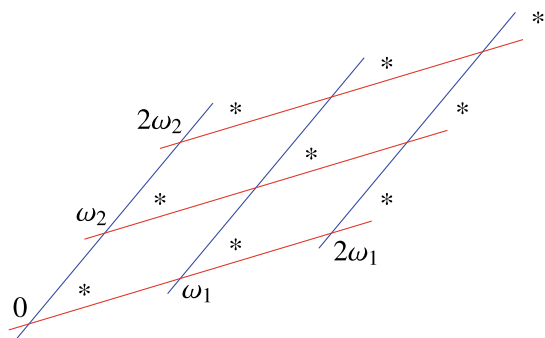


Figure 12.3: Lattice-equivalent points

the equivalent points on its boundary (that is, pasting opposite sides together, as in Figure 12.4). Of course, the torus form of (1) eventually came to light through the Riemann surface construction given in Section 11.8.

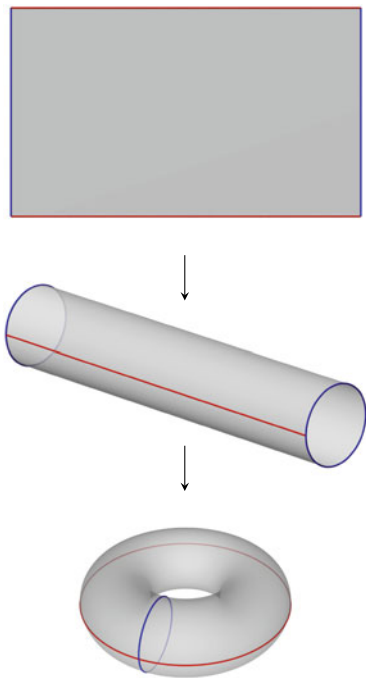


Figure 12.4: Construction of torus by pasting

Weierstrass (1863) elegantly showed both the double periodicity of elliptic functions and the parameterization of cubic curves. Beginning with

$$\sum_{m,n=-\infty}^{\infty} \frac{1}{(z + m\omega_1 + n\omega_2)^2},$$

which is obviously double periodic, he defined the function

$$\wp(z) = \frac{1}{z^2} + \sum_{m,n \neq 0,0}^{\infty} \left(\frac{1}{(z + m\omega_1 + n\omega_2)^2} - \frac{1}{(m\omega_1 + n\omega_2)^2} \right),$$

which has better convergence properties and is also doubly periodic. He then showed by simple computations with series that

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3,$$

where g_2, g_3 are the constants, depending on ω_1, ω_2 , that were defined in Section 12.4. It follows that the point $(\wp(z), \wp'(z))$ lies on the curve

$$y^2 = 4x^3 - g_2x - g_3, \quad (3)$$

and a little further checking shows that (3) is in fact *isomorphic* to \mathbb{C}/Λ , where Λ is the lattice of periods of \wp . The parameterization of all curves (1) by elliptic functions follows by making a linear transformation.

The reason for saying that the curve and \mathbb{C}/Λ are isomorphic (which comes from the Greek for “same form”) is not only because they both have the form of a torus. They also have the same *algebraic structure*, which comes to light when we consider their natural *addition* operation.

Once the curve (1) is parameterized as

$$x = f(z), \quad y = f'(z),$$

the “addition” of points on the curve is induced by adding their parameter values. By the double periodicity of f and f' , this “addition” is simply ordinary addition in \mathbb{C} , modulo Λ . In particular, it is immediate that addition of points has some properties of ordinary addition, such as commutativity and associativity. However, as mentioned in Section 10.3, addition of parameter values z is also reflected in the geometry of the curve. The most concise statement of the relationship, due to Clebsch (1864), is that if z_1, z_2, z_3 are parameter values of three collinear points, then

$$z_1 + z_2 + z_3 = 0 \pmod{(\omega_1, \omega_2)}$$

(or $z_1 + z_2 + z_3 \in \Lambda$). This means that addition of points also has an elementary geometric interpretation, for which, incidentally, the algebraic properties are far less obvious.

On the other hand, the straight-line interpretation of addition gives the simplest explanation of the addition theorems for elliptic functions. As we saw in Section 10.3, the value of $f(z_3)$ is easy to compute as a rational function of $f(z_1)$, $f'(z_1)$, $f(z_2)$, $f'(z_2)$ when z_1, z_2, z_3 are the parameter values of collinear points. Originally, of course, the formula was obtained by Euler, with great difficulty, by manipulating the integral inverse to f (see Section 10.7).

Another reason to accept \mathbb{C}/Λ as the “right” view of the curve is that it answers the seemingly unrelated question of classification by projective equivalence. Recall from Section 7.4 that Newton reduced cubics to the cusp type, the double-point type, and three nonsingular types using real projective transformations. All cubics with a cusp are, in fact, equivalent to $y^2 = x^3$, and all with a double point are equivalent to $y^2 = x^2(x + 1)$, while the distinction between the nonsingular types disappears over the complex numbers, where, as we now know, all are equivalent to tori \mathbb{C}/Λ . The problem that remains is to decide projective equivalence *among* the nonsingular cubics. Salmon (1851) showed that this was determined by a certain complex number τ , which can be computed from the equation of the curve. He defined τ geometrically, so that its projective invariance was obvious, with no thought of elliptic functions. But τ turned out to be nothing but ω_1/ω_2 , which means that two nonsingular cubics are projectively equivalent if and only if their period lattices Λ have the same shape.

EXERCISES

Strictly speaking, the ratio $\tau = \omega_1/\omega_2$ determines only the shape of the *parallelogram* with vertices $0, \omega_1, \omega_2$, and $\omega_1 + \omega_2$.

- 12.5.1** Explain how both the angle between adjacent sides of this parallelogram, and the ratio between their lengths, may be extracted from $\tau = \omega_1/\omega_2$.

The lattice of periods

$$\Lambda = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$$

can be viewed as the set of vertices in a tiling of the plane by copies of this parallelogram, as in Figure 12.3. However, infinitely many *differently shaped parallelograms* give the same Λ . Thus the number τ alone should not be taken to characterize the shape of Λ .

- 12.5.2** Show that Λ may also be tiled by copies of a parallelogram with shape given by $\tau + 1$.
- 12.5.3** More generally, show that Λ may be generated by any two of its elements, $\omega'_1 = a\omega_1 + b\omega_2$ and $\omega'_2 = c\omega_1 + d\omega_2$ provided $ad - bc = \pm 1$. *Hint:* Write down a product of matrices transforming the column vector of (ω_1, ω_2) to (ω'_1, ω'_2) and back to (ω_1, ω_2) , and take its determinant.
- 12.5.4** Deduce from Exercise 12.5.3 that the lattice $\Lambda = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$ has shape characterized by the whole family of complex numbers

$$\frac{a\tau + b}{c\tau + d} \quad \text{where} \quad \tau = \frac{\omega_1}{\omega_2} \quad \text{and} \quad a, b, c, d \text{ are integers with } ad - bc = \pm 1.$$

There are functions of the complex variable τ that depend only on the lattice Λ , and hence take the same value for each number $(a\tau + b)/(c\tau + d)$ characterizing the lattice shape.

- 12.5.5** Consider g_2 and g_3 from Section 12.4, which are obviously functions $g_2(\Lambda)$ and $g_3(\Lambda)$ of the lattice Λ . Show that g_2^3/g_3^2 and $g_2^3/(g_3^3 - 27g_2^2)$ are both functions of τ .

The latter function is none other than the famous *modular function* mentioned in Section 5.7 in connection with the solution of the quintic equation. For more on its amazing properties, see McKean and Moll (1997).

12.6 Uniformization

The characteristic of nonsingular cubics that allows their parameterization by elliptic functions is their topological form. The two periods correspond to the two essentially different circuits around the torus (Figure 12.2).

A representation of the x and y values on a curve by simultaneous functions of a single parameter z is sometimes called a *uniform* representation, and so the problem of parameterizing all algebraic curves in this way came to be known as the *uniformization* problem. Once the elliptic case was understood, it became clear that a solution of the uniformization problem for arbitrary algebraic curves would depend on a better understanding of surfaces: their topology, the periodicities associated with their closed curves, and the way these periodicities could be reflected in \mathbb{C} . These problems were first attacked by Poincaré and Klein in the 1880s, and their work led to the eventual positive solution of the uniformization problem by Poincaré (1907) and Koebe (1907).

Even more important than the solution of this single problem, however, was the amazing convergence of ideas in the preliminary work of Poincaré and Klein. They discovered that multiple periodicities are reflected in \mathbb{C} by groups of transformations, and that the transformations in question are of the simple type $z \mapsto (az + b)/(cz + d)$, called *linear fractional*. We first met these transformations, for a real variable, as transformations of the projective line in Section 7.6.

Linear fractional transformations generalize the linear transformations $z \mapsto z + \omega_1$, $z \mapsto z + \omega_2$ naturally associated with the periods of elliptic functions. However, while the transformations $z \mapsto z + \omega_1$, $z \mapsto z + \omega_2$ are algebraically and geometrically transparent—they commute, and they generate the general transformations $z \mapsto z + m\omega_1 + n\omega_2$, which are simply translations of the plane—the more general linear fractional transformations are not as easily understood. Linear fractional transformations do not normally commute, and their mastery requires a simultaneous grasp of algebraic, geometric, and topological aspects.

The simultaneous view was enormously fruitful in the development of group theory and topology, as we will see in Chapters 14 and 15. Geometry also got a new lease of life when Poincaré (1882) found that linear fractional transformations give an interpretation of non-Euclidean geometry, a field that until then had been a curiosity on the fringes of mathematics. In the next chapter we look at the origins of non-Euclidean geometry and see how the subject was transformed by Poincaré's discovery.

EXERCISES

The first example, beyond the elliptic functions, of periodicity under linear fractional transformations is seen in the modular function derived in the previous exercise set. It turns out that the periodicity of the modular function can be generated by two transformations: $z \mapsto z + 1$ and $z \mapsto -1/z$. This periodicity can be depicted by a pattern shown in Figure 13.20.

12.6.1 Check that $z \mapsto z + 1$ and $z \mapsto -1/z$ are among the transformations

$$z \mapsto \frac{az + b}{cz + d}, \quad \text{where } a, b, c, d \text{ are integers with } ad - bc = \pm 1.$$

12.6.2 Show that the transformations $z \mapsto z + 1$ and $z \mapsto -1/z$ do not commute.

12.6.3 Show that both $z \mapsto z + 1$ and $z \mapsto -1/z$ map the half-plane $\{\operatorname{Im} z > 0\}$ onto itself, and that $z \mapsto -1/z$ exchanges the inside and outside of the unit circle.



13

Non-Euclidean Geometries

PREVIEW

One of the new frontiers in geometry opened up by calculus was the study of *curvature*. The concept of curvature is particularly interesting for surfaces, because it can be defined *intrinsically*. The intrinsic curvature, or *Gaussian* curvature as it is known, is unaltered by bending the surface, so it can be defined without reference to the surrounding space.

This leads to the study of *intrinsic* surface geometry, in which distance, “lines” (curves of shortest length), angles, areas, and so on, are defined by measurements within the surface.

The question then arises, to what extent does the intrinsic geometry of a curved surface resemble the classical geometry of the plane? For surfaces of *constant* curvature, the difference is reflected in two of Euclid’s axioms: the axiom that straight lines are infinite, and the parallel axiom.

On surfaces of constant positive curvature, such as the sphere, all lines are finite and there are no parallels. On surfaces of zero curvature there may also be finite straight lines; but if all straight lines are infinite the parallel axiom holds. The most interesting case is constant negative curvature because it leads to a realization of *non-Euclidean geometry*, found by Beltrami (1868a).

Poincaré (1882) showed that some of Beltrami’s realizations arise naturally in complex analysis. Papers had already been published with pictures of patterns of non-Euclidean “lines,” most notably Schwarz (1872). Thus, non-Euclidean geometry was actually a part of existing mathematics, but a part whose geometric nature had not previously been understood.

13.1 Transcendental Curves

We saw in Chapter 8 that calculus in the 17th century was greatly stimulated by problems in the geometry of curves. Differentiation grew from methods for constructing tangents, and integration from attempts to find areas and arc lengths. Not only did calculus unlock the secrets of the classical curves and of the algebraic curves defined by Descartes; it also extended the concept of curve itself. Once it became possible to handle slopes, lengths, and areas with precision, it also became possible to use these quantities to define new, nonalgebraic, curves. These were the curves called “mechanical” by Descartes (Section 6.3) and “transcendental” by Leibniz. In contrast to algebraic curves, which could be studied in some depth by purely algebraic methods, transcendental curves were inseparable from the methods of calculus. Hence it is not surprising that a new set of geometric ideas, the ideas of “infinitesimal” or *differential* geometry, emerged from the investigation of transcendental curves.

Among the new results on transcendental curves was the first solution of the ancient problem of arc length. The problem was first posed for an algebraic curve, the circle, by the Greeks and in this case it is equivalent to an area problem (“squaring the circle”), since both area and arc length of the circle depend on π . As we now know, π is a transcendental number (Section 2.3), so the arc length problem for the circle has no solution by the elementary means allowed by the Greeks. The first curve whose arc length could be found by elementary means was discovered by Harriot around 1590. It is the curve defined by the polar equation

$$r = e^{k\theta}$$

known as the *logarithmic* or *equiangular* spiral.

Harriot did not have the exponential function and knew the curve only by its equiangular property, which is that the tangent makes a constant angle α (depending on k) with the radius vector. The spiral turned up in his researches on navigation and map projections (Section 12.2) as the plane projection of a *rhumb line* on the sphere. A rhumb line is a curve that meets the meridians at a constant angle; in practical terms, it represents the course of a ship sailing in a fixed compass direction.

Not having the tools of calculus, Harriot relied on ingenious geometry and a simple limit argument, which was brought to light by Lohne (1979). The idea should be clear from Figure 13.1.

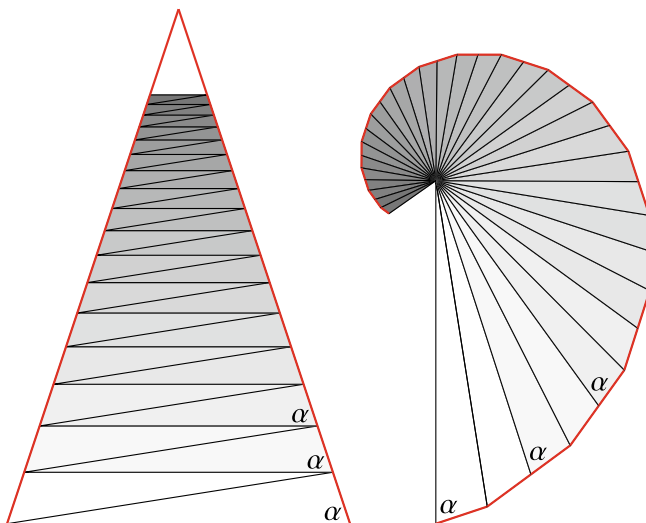


Figure 13.1: Harriot's construction of the equiangular spiral

An equilateral triangle with base angles α is cut into similar trapezoids by lines parallel to its base. When each trapezoid is cut by its diagonal, the resulting triangles can be reassembled into a kind of fan bounded by a polygonal spiral consisting of pieces of the red sides of the original triangle. The red spiral is equiangular in the sense that every other line from the common apex of the triangles meets it at angle α .

When the construction is continued indefinitely, it is obvious that the total length of the red spiral is the sum of the red sides of the triangle. This is true *independently of the height of the trapezoids*. Now, if we let the height of the trapezoids approach zero, the polygonal spiral approaches a smooth equiangular spiral, whose length therefore equals the sum of the red sides of the triangle.

Harriot's work was not published, and the arc length of the equiangular spiral was rediscovered by Torricelli (1645). Gradually the problem of arc length became understood more systematically as a problem of integration, though usually a rather intractable one. The first solution for an algebraic curve was for the "semicubical parabola" $y^2 = x^3$, by Neil and Heuraet in 1657. Soon after this Wren¹ solved the problem for the cycloid, the path traced by a point on a circle rolling on a line. His solution was

¹This is none other than Sir Christopher Wren, famous for designing many churches in London, such as St Paul's cathedral.

given by Wallis (1659). Wren found, remarkably, that the length of one arch of the cycloid is a rational multiple (namely, 4) of the diameter of the circle.

Other remarkable properties of the cycloid are related to mechanics, and one of these will be seen geometrically in the next section. Another among the first known transcendental curves is the *tractrix* of Newton (1676b). Newton defined this curve by the property that the length of its tangent from point of contact to the x -axis is constant (Figure 13.2).

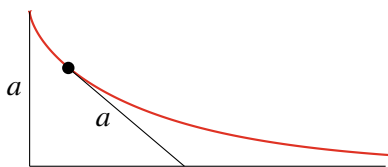


Figure 13.2: The tractrix

It follows that the tractrix satisfies

$$\frac{dy}{ds} = \frac{y}{a},$$

where s denotes arc length. By using $ds = \sqrt{dx^2 + dy^2}$, this differential equation can be solved to give

$$x = a \log \frac{a + \sqrt{a^2 - y^2}}{y} - \sqrt{a^2 - y^2},$$

the equation for the curve given, in more geometric language, by Huygens (1693b). Huygens pointed out that the curve could be interpreted as the path of a stone pulled by a string of length a (hence the name “tractrix”). Thus the tractrix, too, has some mechanical significance. In fact it can be constructed from a famous mechanical curve, the *catenary*, which is the shape of a hanging chain. The method is described in the next section. But the most important role of the tractrix is to generate the *pseudosphere*, a surface of constant negative curvature discussed in Section 13.3.

EXERCISES

The arc length of $y^2 = x^3$ is today a fairly routine exercise with the arc length integral $\int \sqrt{1 + \left(\frac{dy}{dx}\right)^2} dx$.

13.1.1 Show that the arc length of $y = x^{3/2}$ between O and $x = a$ is

$$\frac{8}{27} \left(\left(1 + \frac{9a}{4} \right)^{3/2} - 1 \right).$$

Likewise, it is easy for us to derive properties of the logarithmic spiral from its polar equation and knowledge of the exponential function.

13.1.2 Show that the logarithmic spiral is *self-similar*. That is, magnifying $r = e^{k\theta}$ by a factor m to $r = me^{k\theta}$ gives a curve that is congruent to the original (in fact, it results from a rotation of the original).

Jakob Bernoulli was so impressed by this property of the logarithmic spiral that he arranged to have the spiral engraved on his tombstone, with a motto: *Eadem mutata resurgo* (“Though changed, I arise again the same”). (See Jakob Bernoulli (1692) p. 213.)

13.1.3 Deduce the equiangular property of the logarithmic spiral from its self-similarity.

The equation of the tractrix given above can be derived as follows.

13.1.4 Explain why the constant tangent property implies $\frac{dy}{ds} = \frac{y}{a}$, then multiply both sides of this equation by $\frac{ds}{dx} = \sqrt{1 + \left(\frac{dy}{dx}\right)^2}$, and deduce that

$$\frac{dx}{dy} = \pm \frac{\sqrt{a^2 - y^2}}{y}.$$

13.1.5 Check by differentiation that $x = a \log \frac{a + \sqrt{a^2 - y^2}}{y} - \sqrt{a^2 - y^2}$ satisfies the differential equation found in Exercise 13.1.4, and also show that x has the appropriate value when $y = a$.

13.2 Curvature of Plane Curves

As mentioned at the beginning of this chapter, *curvature* is one of the most important ideas in differential geometry. The extension of this idea from curves to surfaces and then to higher-dimensional spaces has had many important consequences for mathematics and physics, among them clarification of both the mathematical and physical meaning of “space,” “space-time,” and “gravitation.” In this section we look at the beginnings of the theory of curvature in the 17th-century theory of curves.

Just as the direction of a curve C at point P is determined by its straight-line approximation, that is, tangent, at P , the curvature of C at P is determined by an approximating circle. Newton (1665c) was the first to single

out the circle that defines the curvature: the circle through P whose center R is the limiting position of the intersection of the normal through P and the normal through a nearby point Q on the curve. R is called the *center of curvature*, $RP = \rho$ the *radius of curvature*, and $1/\rho = \kappa$ the *curvature*. It follows that the circle of radius r has constant curvature $1/r$. The only other curve of constant curvature is the straight line, which has curvature 0. This follows from the formula for curvature discovered by Newton (1671):

$$\rho = \frac{[1 + (dy/dx)^2]^{3/2}}{d^2y/dx^2}.$$

There is an interesting relationship between a curve C and the locus C' of the center of curvature of C . C is the so-called *involute* of C' , which, intuitively speaking, is the path of the end of a piece of string as it is unwound from C' (Figure 13.3). It is intuitively clear that Q , the end of the string, is instantaneously moving in a circle with center at P , the point where the string is tangential to C' .

Huygens discovered that the involute of a cycloid is *another cycloid*—a property used in Huygens (1673) to design clocks with a *cycloidal pendulum*. (Thus if the blue curve above is replaced by a cycloid, a weight Q on the end of a string PQ swings in a cycloidal path which, by another result of Huygens, takes constant time.) Two other stunning results on involutes are due to the Bernoulli brothers. Jakob Bernoulli (1692) found that the involute of the logarithmic spiral is another logarithmic spiral, and Johann Bernoulli (1691) found that the tractrix is the involute of the catenary, $y = \cosh x$.

EXERCISES

Despite the complexity of the Newton curvature formula, it is easy enough to solve for y when the curvature κ is zero.

13.2.1 Use the formula to show that $\kappa = 0$ implies that y is a linear function of x .

13.2.2 Show that $d\theta/ds = 1/r$ for the circle of radius r , and deduce that $d\theta/ds = \kappa$ for any curve.

The description of the tractrix as the involute of the catenary is convenient for studying the pseudosphere. We therefore work out some steps in this approach in the following exercises. The curve C' in Figure 13.3 is now assumed to be the catenary $y = \cosh x$, which meets the y -axis at the point S where $y = 1$.

13.2.3 Using the arc length integral on the catenary $y = \cosh x$ between $S = (0, 1)$ and $P = (\sigma, \cosh \sigma)$, show that

$$\text{arc length } PS = \sinh \sigma = PQ.$$

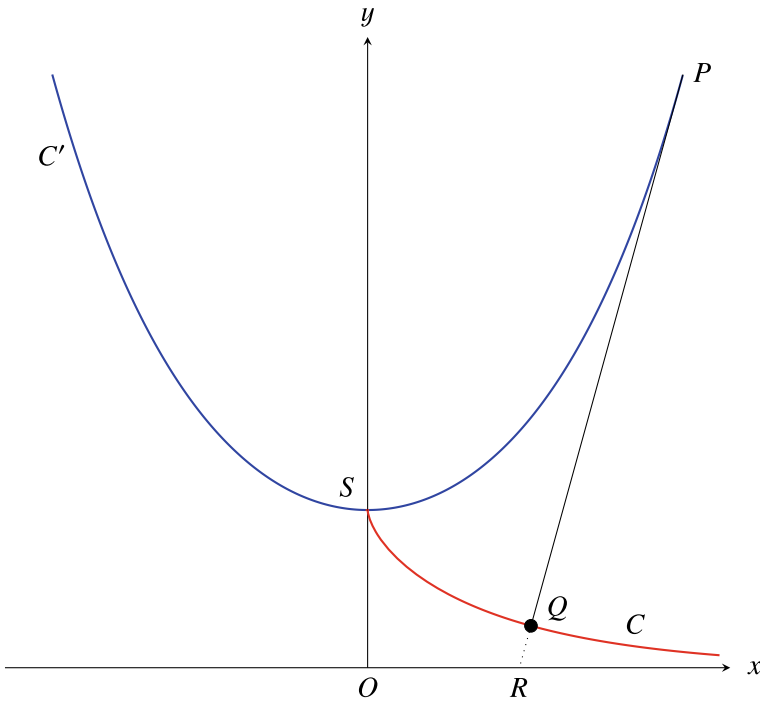


Figure 13.3: Construction of the involute

13.2.4 Also find the equation of the tangent at P , and use it to show that $R = (\sigma - \coth \sigma, 0)$. Then use the value of PQ to show that

$$QR = \frac{1}{\sinh \sigma} = \frac{1}{PQ}.$$

13.2.5 Finally, use the length of PQ again to show that $Q = (\sigma - \tanh \sigma, \operatorname{sech} \sigma)$, and show that the parametric equations of the tractrix C ,

$$x = \sigma - \tanh \sigma, \quad y = \operatorname{sech} \sigma,$$

imply the cartesian equation of the tractrix (with $a = 1$),

$$x = \log \frac{1 + \sqrt{1 - y^2}}{y} - \sqrt{1 - y^2}.$$

13.3 Curvature of Surfaces

The first approach to defining curvature at a point P of a surface S was to express it in terms of the curvature of plane curves, by considering sections of S by planes through the normal at P . Of course, different planes normal to the surface at P may cut the surface in quite different curves, with different curvatures, as the example of the cylinder shows (Figure 13.4).

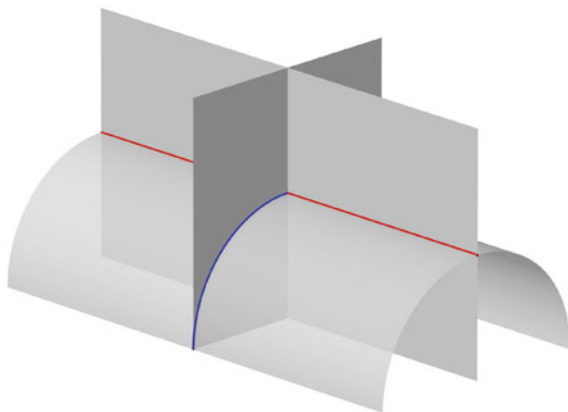


Figure 13.4: Sections of the cylinder

However, among these curves there will be one of maximum curvature and one of minimum curvature (which may be negative, if we give a sign to curvature according to the side on which the center of curvature lies). Euler (1760) showed that these two curvatures κ_1 and κ_2 , called the *principal curvatures*, occur in perpendicular sections and that together they determine the curvature κ in a section at angle α to one of the principal sections by

$$\kappa = \kappa_1 \cos^2 \alpha + \kappa_2 \sin^2 \alpha.$$

This is where we are led when the curvature of surfaces is subordinated to the curvature of curves. A deeper idea occurred to Gauss while he was working in geodesy (surveying and mapmaking): curvature of a surface may be detectable *intrinsically*, that is, by measurements entirely within the surface. The curvature of the earth, for example, was known from measurements made by explorers and surveyors, *not* (in the time of Gauss) by viewing it from space. Gauss (1827) made the extraordinary discovery that the quantity $\kappa_1 \kappa_2$ can be defined intrinsically and hence can serve as an

intrinsic measure of curvature. He was so proud of this result that he called it the *theorema egregium* (excellent theorem). It follows in particular that $\kappa_1\kappa_2$, which is called the *Gaussian curvature*, is unaffected by bending.

The plane, for example, has $\kappa_1 = \kappa_2 = 0$ and thus zero Gaussian curvature. Hence so has any surface obtained by bending a plane, such as a cylinder. We can verify the *theorema egregium* in this case, because one of the principal curvatures of a cylinder is obviously zero.

Surfaces S_1, S_2 obtained from each other by bending are said to be *isometric*. More precisely, S_1 and S_2 are isometric if there is a one-to-one correspondence between points P_1 of S_1 and points P_2 of S_2 such that

$$\text{distance between } P_1 \text{ and } P'_1 \text{ in } S_1 = \text{distance between } P_2 \text{ and } P'_2 \text{ in } S_2,$$

where the distances are measured *within* the respective surfaces. A more precise statement of the *theorema egregium* then is: *if S_1, S_2 are isometric, then S_1, S_2 have the same Gaussian curvature at corresponding points.*

Surfaces of Constant Curvature

The simplest surface of constant positive curvature is the sphere of radius r , which has curvature $1/r^2$ at all points. Other surfaces of curvature $1/r^2$ may be obtained by bending portions of the sphere; however, all such surfaces have either edges or points where they are not smooth, as was proved by Hilbert (1901). The plane, as we have seen, has zero curvature, and so have all surfaces obtained by bending the plane or portions of it.

It remains to investigate whether there are surfaces of constant *negative* curvature. In ordinary space, such a surface has principal curvatures of opposite sign at each point, so it looks locally like a saddle (Figure 13.5).

Several surfaces of constant negative curvature were given by Minding (1839). The most famous of them is the *pseudosphere*, the surface of revolution obtained by rotating a tractrix about the x -axis (Figure 13.6). This surface was investigated as early as 1693 by Huygens, who found its surface area, which is finite, and the volume and center of mass of the solid it encloses, which are also finite (Huygens (1693a)).

The pseudosphere, despite the “sphere” part of its name, is more like a negative-curvature counterpart of the cylinder. So one may wonder whether a surface of constant negative curvature can be more like a plane. Hilbert (1901) proved that no smooth unbounded surface of constant negative curvature lies in ordinary space, so this rules out planelike surfaces and also

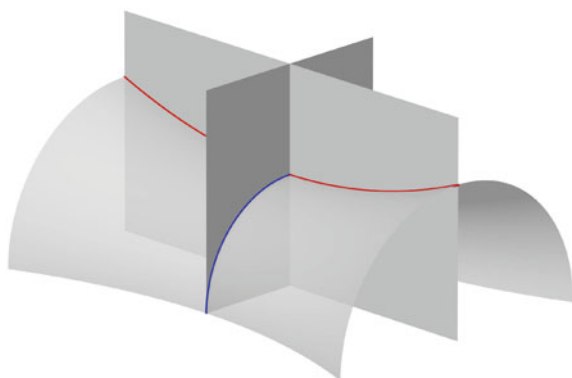


Figure 13.5: A saddle

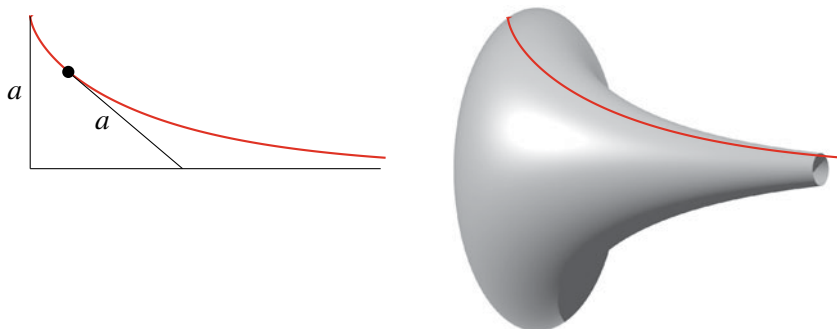


Figure 13.6: The tractrix and the pseudosphere

accounts for the “edge” on the pseudosphere (where, in fact, the curvature of the tractrix becomes infinite). One can, however, make a “plane” of negative curvature by using a nonstandard notion of length in the Euclidean plane. This discovery of Beltrami (1868a) is discussed in Section 13.7, along with other implications of negative curvature for non-Euclidean geometry.

These geometric implications can also be glimpsed if we ask whether surfaces S_1 , S_2 of equal curvature are isometric. Even with zero curvature this is false, since a plane is not isometric to a cylinder. What *is* true, though, is that any sufficiently small portion of the plane can be mapped isometrically into any part of the cylinder. Minding (1839) showed that

the same is true for any two surfaces S_1, S_2 of equal constant curvature. Taking $S_1 = S_2$, this says that *rigid motion* is possible in S_1 : a body in S_1 can be moved, without any shrinking or stretching, to any part of S_1 large enough to contain it. The latter restriction is necessary, for example, for the pseudosphere since it becomes arbitrarily narrow as $x \rightarrow \infty$.

The possibility of rigid motion was fundamental to Euclid's geometry of the plane, and with the discovery of curved surfaces that support rigid motion, Euclid's geometry could be seen as a special case—the zero curvature case—of something broader. The broader notion of geometry on a surface begins to take shape once one has an appropriate notion of “straight line.” This is developed in the next section.

EXERCISES

The construction of the tractrix as the involute of the catenary in Section 13.2 gives a remarkable insight into the two principal curvatures of the pseudosphere, enabling us to see why the pseudosphere has constant negative curvature.

13.3.1 Interpreting PQ in Figure 13.3 as the radius of curvature of the tractrix, and hence as the curvature of a section of the pseudosphere, suggest an interpretation of QR as a radius of curvature.

13.3.2 Assuming that PQ and QR are in fact principal radii of curvature, deduce from Exercise 13.2.4 that

Gaussian curvature of the pseudosphere at any point = -1 .

13.4 Geodesics

A “straight line” on a surface, or *geodesic* as it is called, can be defined equivalently by a shortest-distance property or a zero-curvature property. The shortest-distance definition has the drawback that a geodesic is *not* necessarily the shortest path between two points. On a sphere, for example, there are two geodesics between two nearby points P_1, P_2 : the short portion and the long portion of the great circle through P_1, P_2 . What is true is that the geodesic gives the shortest distance between any two of its points that are sufficiently close together. Even so, it is generally hard to find *which* curve between given points on a surface has minimum length. Nevertheless, this is how geodesics were first defined, by Jakob and Johann Bernoulli; and Euler (1728a) found a differential equation for geodesics from this approach.

A more elementary approach is to define the *geodesic curvature* κ_g at P of a curve C on a surface S as the ordinary curvature of the orthogonal projection of C in the tangent plane to S at P . As one might expect, geodesic curvature can also be defined intrinsically, and κ_g was introduced in this way by Gauss (1825). A geodesic is then a curve of zero geodesic curvature. This is the definition of Bonnet (1848).

The latter definition immediately shows that great circles on the sphere are geodesics, since their projections onto tangent planes are straight lines. Other examples are the horizontal lines, vertical circles, and helices on the cylinder (Figure 13.7). These all come from straight lines on the plane that is rolled up to form the cylinder.

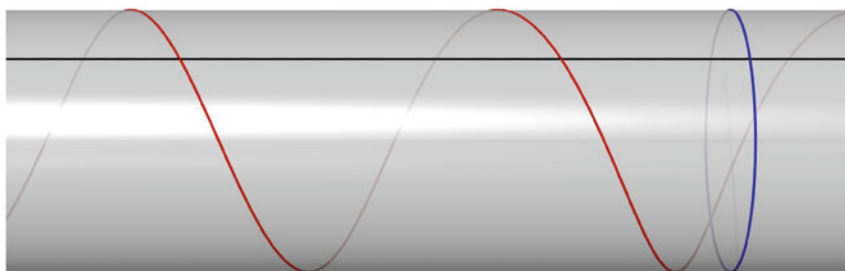


Figure 13.7: Geodesics on the cylinder

Geodesics on the pseudosphere, and other surfaces of negative curvature, are not all so simple to describe. However, Section 13.8 shows that they become simple when one maps the surface of constant negative curvature suitably onto a plane.

EXERCISES

- 13.4.1** Are the circles on the pseudosphere, in planes perpendicular to its axis, geodesics? Give a qualitative argument to support your answer.

It may be easier to answer this question if one first considers the *cone*, a surface also obtained by bending the plane. To avoid worrying about the apex, where the cone is not smooth, we omit this point.

- 13.4.2** Show that the circles on the cone, in planes perpendicular to its axis, are *not* geodesics.
- 13.4.3** Show that there are nonsmooth geodesics on the cone, that is, curves of geodesic curvature zero except at certain points where they have no tangent.

13.5 The Parallel Axiom

Until the 19th century, Euclid's geometry enjoyed absolute authority, both as an axiomatic system and as a description of physical space. Euclid's proofs were regarded as models of logical rigor, and his axioms were accepted as correct statements about physical space. Even today, Euclidean geometry is the simplest type of geometry, and it furnishes the simplest description of physical space for everyday purposes. Beyond the everyday world, however, lies a vast universe that can be understood only with the help of an expanded geometry. The expansion of geometric concepts began with doubts about one of Euclid's axioms, the *parallel axiom*.

For our purposes, the most convenient statement of the parallel axiom is as follows:

Axiom P_1 . For each straight line L and point P outside L there is exactly one line through P that does not meet L .

There are many other equivalent statements of Axiom P_1 , some obviously fairly close to it, for example, Euclid's own from Section 2.1:

That if a straight line falling on two straight lines make the interior angles on the same side less than two right angles, the two straight lines, if produced indefinitely, meet on that side on which are the angles less than the two right angles.

Heath (1925), p. 202

Other equivalents of Axiom P_1 are less obviously so. For example,

- (i) The angle sum of a triangle = π (Euclid).
- (ii) The locus of points equidistant from a straight line is a straight line. (al-Haytham, around 1000 CE).
- (iii) Similar triangles of different sizes exist (Wallis (1663); see Fauvel and Gray (1988), p. 510).

Thus a denial of the parallel axiom entails denial of (i), (ii), and (iii). A denial of (iii) means in particular that scale models are impossible, since three points in the original object and the three corresponding points of a scale model would define similar triangles of different sizes.

Such unlikely consequences convinced many people that the parallel axiom was a logically necessary property of straight lines, already implied by the other axioms of Euclid, and so efforts were made to prove it outright.

The most tenacious attempt, entitled *Euclides ab omni naevo vindicatus* (Euclid cleared of every flaw), was made by Saccheri (1733). Saccheri's plan of attack began by subdividing the denial of the parallel axiom into two alternatives:

Axiom P_0 . There is no line through P that does not meet L .

Axiom P_2 . There are at least two lines through P that do not meet L .

The next step was to destroy each alternative by deducing a contradiction from it. He succeeded in deducing a contradiction from Axiom P_0 , using other axioms of Euclid, such as the axiom that a straight line can be prolonged indefinitely. (Such additional assumptions are certainly necessary, since great circles on the sphere have some properties of straight lines, except that they are finite in length.)

Saccheri was less successful with Axiom P_2 . The consequences he derived from it, hoping to obtain a contradiction, were as follows. Among the lines M through P that do not meet L are two extremes, M^+ or M^- , called *parallels* or *asymptotic lines* (Figure 13.8); any of these lines M strictly between M^+ and M^- has a common perpendicular with L and, moreover, the position of this perpendicular tends to infinity as M tends to M^+ or M^- . Although curious, these consequences of Axiom P_2 were not contradictory and Saccheri, sensing that the contradiction was slipping away from him, tried to overtake it by proceeding to infinity.

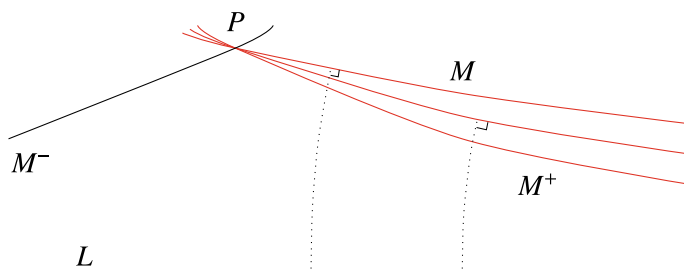


Figure 13.8: Asymptotic lines

He claimed that M^+ would meet L at infinity and have a common perpendicular with it there. But this *still* was not a contradiction. Saccheri

merely claimed that such a conclusion was “repugnant to the nature of the straight line” (Saccheri (1733), p. 173), perhaps visualizing an intersection like Figure 13.9. But why should asymptotic lines not be tangential at infinity? History was to show that this was an appropriate resolution of Saccheri’s “contradiction” (see Section 13.8). Thus Saccheri’s results were not, as he thought, steps toward a proof of the parallel axiom; they were the first theorems of a *non-Euclidean* geometry in which Axiom P_2 replaces the parallel axiom.

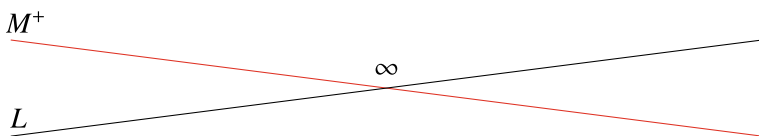


Figure 13.9: Hypothetical intersection at infinity

EXERCISES

The connection between the parallel axiom and the angle sum of a triangle is very direct and elegant.

13.5.1 Deduce, from Euclid’s version of the parallel axiom, that a line falling on two *parallel* lines makes interior angles that sum to π .

13.5.2 Use Exercise 13.5.1 and the construction in Figure 13.10 (in which CD is parallel to AB) to show that $\alpha + \beta + \gamma = \pi$.

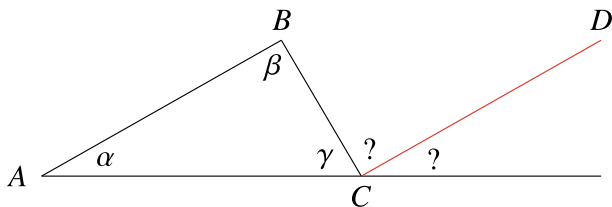


Figure 13.10: The angle sum of a triangle

13.5.3 Deduce from Exercise 13.5.2 that the angle sum of any quadrilateral is 2π and, in particular, that squares exist.

Thus theorems mentioning squares, such as the Pythagorean theorem, can hold only when Euclid’s parallel axiom is assumed.

13.6 Spherical and Hyperbolic Geometry

In rejecting P_0 because of its incompatibility with infinite lines, Saccheri ruled out the most natural geometry in which P_0 holds, that of the sphere with great circles as “lines.” Spherical geometry had been cultivated since ancient times by astronomers and navigators, and formulas for the side lengths and areas of spherical triangles were well known. For the history of this now-neglected subject, see Van Brummelen (2013). But the sphere was considered part of Euclid’s spatial geometry, so the axiomatic significance of spherical geometry was initially ignored. However, spherical geometry did guide the first explorations of Axiom P_2 .

Lambert (1766) made the striking discovery that Axiom P_2 implies that the area of a triangle with angles α, β, γ is proportional to $\pi - (\alpha + \beta + \gamma)$, its angular defect. In other words,

$$\text{area} = -R^2(\alpha + \beta + \gamma - \pi)$$

for some positive constant R^2 . Having rediscovered the theorem (Exercise 13.6.5 below) that, for a triangle on the sphere of radius R ,

$$\text{area} = R^2(\alpha + \beta + \gamma - \pi),$$

Lambert mused that one “could almost conclude that the new geometry would be true on a sphere of imaginary radius.” What a sphere of radius iR might be was unclear, but the idea that complex numbers can give the formulas of a hypothetical geometry proved fruitful.

It was found that formulas implied by Axiom P_2 are obtained from the corresponding formulas of spherical geometry replacing R by iR . This amounts to replacing circular functions by hyperbolic functions. For example, Gauss (1831) deduced from Axiom P_2 that the circumference of a circle of radius r is $2\pi R \sinh r/R$. The same expression follows by replacing R by iR in $2\pi R \sin r/R$, which is the circumference of a circle of radius r on the sphere of radius R (where, of course, r is measured *on* the spherical surface; see the red circle in Figure 13.11 and Exercise 13.6.1).

Lambert (1766) introduced the hyperbolic functions and noted their analogy with the circular functions, but he did not follow through with a complete translation of spherical formulas into hyperbolic formulas. This was first done by Taurinus (1826), one of a small circle who corresponded with Gauss on geometric questions.

The formulas gave the geometry of Axiom P_2 a second leg to stand on, but there was still nothing solid under its feet. Neither Gauss nor Taurinus seemed confident of finding an *interpretation* of the formulas. Gauss's student Minding (1840) even showed that the hyperbolic formulas for triangles hold on the pseudosphere, but no one at that time commented on the likely importance of this result. Perhaps it was clear that the pseudosphere cannot serve as a “plane,” because it is infinite in only one direction.

Only in 1868, when Beltrami extended the pseudosphere to a true “plane”—a surface locally isometric to the pseudosphere but infinite in all directions—was the new geometry given a firm foundation. Klein (1871) named the geometry of Axiom P_2 *hyperbolic geometry*, and its “plane” is now called the *hyperbolic plane*.

EXERCISES

- 13.6.1** Prove that the circumference of the circle C of radius r on the sphere of radius R (Figure 13.11) is $2\pi R \sin(r/R)$.

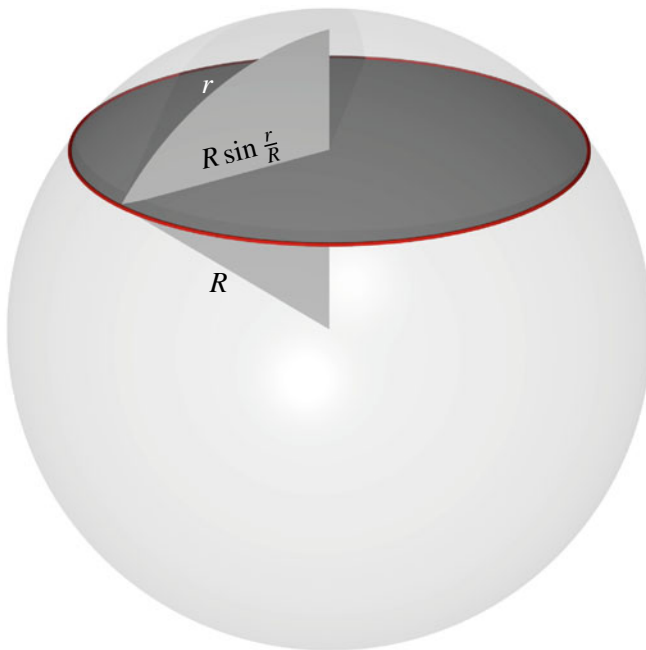


Figure 13.11: Radius and circumference on the sphere

13.6.2 Show that both $2\pi R \sin(r/R)$ and $2\pi R \sinh(r/R)$ tend to $2\pi r$ as $R \rightarrow \infty$.

These results show how even non-Euclidean geometry is “Euclidean in the small”—its formulas tend to the Euclidean formulas as size tends to zero. The same is true of the angle-sum of a triangle, which has a surprising relationship with the area of the triangle.

Figure 13.12 shows a spherical triangle $\Delta_{\alpha\beta\gamma}$ with angles α, β, γ and its sides extended to three great circles. These great circles divide the sphere into eight triangles, in four antipodal pairs. In particular, if the vertices of $\Delta_{\alpha\beta\gamma}$ are A, B, C as shown then their respective antipodal points A', B', C' form a triangle equal to $\Delta_{\alpha\beta\gamma}$.

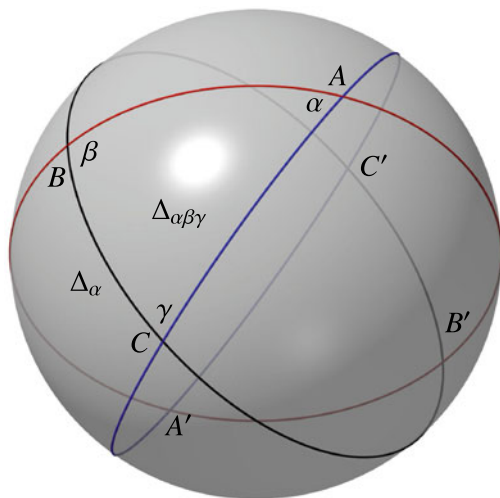


Figure 13.12: Division of sphere by three great circles

The points B, C, A' form a triangle Δ_α which, together with $\Delta_{\alpha\beta\gamma}$, makes a “wedge” of the sphere with angle α (shown in Figure 13.13).

This wedge obviously makes up $\frac{\alpha}{2\pi}$ of the total area S of the sphere, so we can write

$$\Delta_{\alpha\beta\gamma} + \Delta_\alpha = \frac{\alpha}{2\pi} S.$$

13.6.3 If we likewise define spherical triangles $\Delta_\beta = ACB'$ and $\Delta_\gamma = ABC'$ show that

$$\begin{aligned}\Delta_{\alpha\beta\gamma} + \Delta_\beta &= \frac{\beta}{2\pi} S, \\ \Delta_{\alpha\beta\gamma} + \Delta_\gamma &= \frac{\gamma}{2\pi} S,\end{aligned}$$

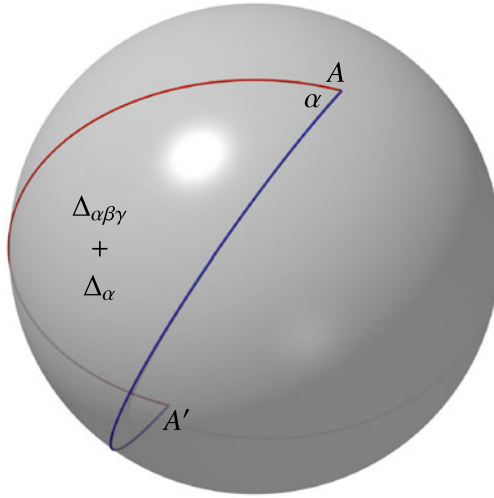


Figure 13.13: Wedge of sphere between two great circles

and hence that

$$3\Delta_{\alpha\beta\gamma} + \Delta_{\alpha} + \Delta_{\beta} + \Delta_{\gamma} = \frac{\alpha + \beta + \gamma}{2\pi} S.$$

13.6.4 Show also that

$$2(\Delta_{\alpha\beta\gamma} + \Delta_{\alpha} + \Delta_{\beta} + \Delta_{\gamma}) = S.$$

13.6.5 Deduce from questions 13.6.3 and 13.6.4 that

$$\Delta_{\alpha\beta\gamma} = \frac{S}{4\pi}(\alpha + \beta + \gamma - \pi),$$

so the area of a spherical triangle with angles α, β, γ is proportional to $\alpha + \beta + \gamma - \pi$. This formula was discovered by Thomas Harriot in 1603.

13.6.6 Deduce from Harriot's area formula that the angle sum of a spherical triangle tends to π as its size tends to zero.

13.7 Geometry of Bolyai and Lobachevsky

The most important contributors to hyperbolic geometry between Gauss and Beltrami were Lobachevsky and Bolyai, who published independent discoveries of the subject: Lobachevsky (1829) and János Bolyai (1832b).

Because of their courage in advocating an unconventional geometry, Bolyai and Lobachevsky have been justly admired. Nevertheless, the immediate impact of their work was slight. Many of their results were already known to Gauss and his circle and could have been picked up from existing publications and personal contacts. Lambert (1766) and Taurinus (1826) were in print, and Bolyai's father, F. Bolyai, was a lifelong friend of Gauss, as was Lobachevsky's teacher Bartels. In any case their work, though more systematic and convincing than previous attempts, attracted very little attention at first. We have seen how the possibility of using differential geometry to justify hyperbolic geometry was overlooked until 1868. Up to that time, there seemed no reason to take hyperbolic geometry seriously.

In retrospect, of course, the theorems of Bolyai and Lobachevsky can be seen to unify the fragmentary results of their predecessors very nicely. They cover the basic relations between sides and angles of triangles (hyperbolic trigonometry), the measure of polygonal areas by angular defect, and formulas for circumference and area of circles. Lobachevsky (1836) broke new ground by finding volumes of polyhedra, which turn out to be far from elementary, involving the function $\int_0^\theta \log 2|\sin t| dt$.

Both Bolyai and Lobachevsky considered a three-dimensional space satisfying Axiom P_2 and made extensive use of a surface peculiar to this space, the *horosphere*. A horosphere is a "sphere with center at infinity," and it is *not* a hyperbolic plane. Wachter, a student of Gauss, observed in a letter of 1816 (published in Stäckel (1901)) that the geometry of the horosphere is in fact Euclidean. This astonishing result was rediscovered by Bolyai and Lobachevsky, and they anticipated that it would make Euclidean geometry subordinate to hyperbolic. We will see in Section 13.8 how this view was vindicated by the work of Beltrami.

Beltrami's Projective Model

Interest in hyperbolic geometry was rekindled in the 1860s when unpublished work of Gauss, who had died in 1855, came to light. Learning that Gauss had taken hyperbolic geometry seriously, mathematicians became more receptive to non-Euclidean ideas. The works of Bolyai and Lobachevsky were rescued from obscurity and, approaching them from the viewpoint of differential geometry, Beltrami (1868a) was able to give them the concrete explanation that had eluded all his predecessors.

Beltrami had studied the geometry of surfaces and found the surfaces that can be mapped onto the plane in such a way that their geodesics go to straight lines (Beltrami (1865)). They turn out to be just the surfaces of constant curvature. In the case of positive curvature, the sphere, such a mapping is central projection onto a tangent plane (Figure 13.14), though of course this maps only half the sphere onto the whole plane.

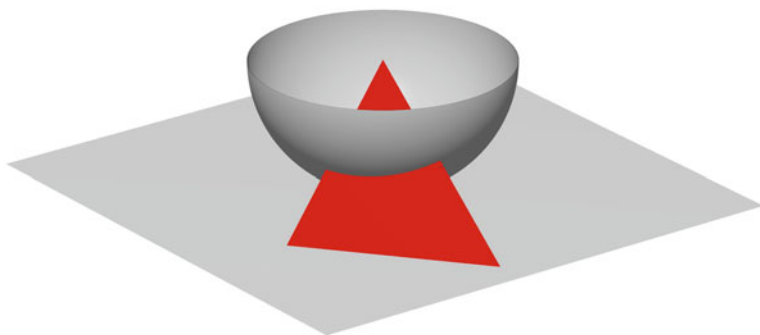


Figure 13.14: Central projection

The mappings of surfaces of constant negative curvature, on the other hand, take the *whole* surface onto only *part* of the plane. Figure 13.15, from Klein (1928), shows some of these mappings (the middle one being of the pseudosphere). The correspondence between the surfaces and their maps is easier to see if one imagines each surface rotated 90° clockwise, so that its geodesics point in roughly the same direction as the straight lines on the map.

Each negatively curved surface S is mapped onto a portion of the unit disk. Beltrami (1868a) realized that the disk can then be viewed as a natural extension of S to an “infinite plane,” thus avoiding the problem of finding “planelike” surfaces of constant negative curvature in ordinary space. Instead one takes the disk as the “plane,” line segments within it as “lines,” and “distance” between two points of the disk as the distance between their preimage points on the surface S . The function $d(P, Q)$, giving “distance” between points P, Q of the disk in this way, turns out to be meaningful for all points inside the unit circle, so the notion of “distance” extends to the whole open disk. As Q approaches the unit circle, $d(P, Q)$ tends to infinity, so the “plane,” and hence the “lines” in it, are indeed infinite with respect to this nonstandard “distance.”

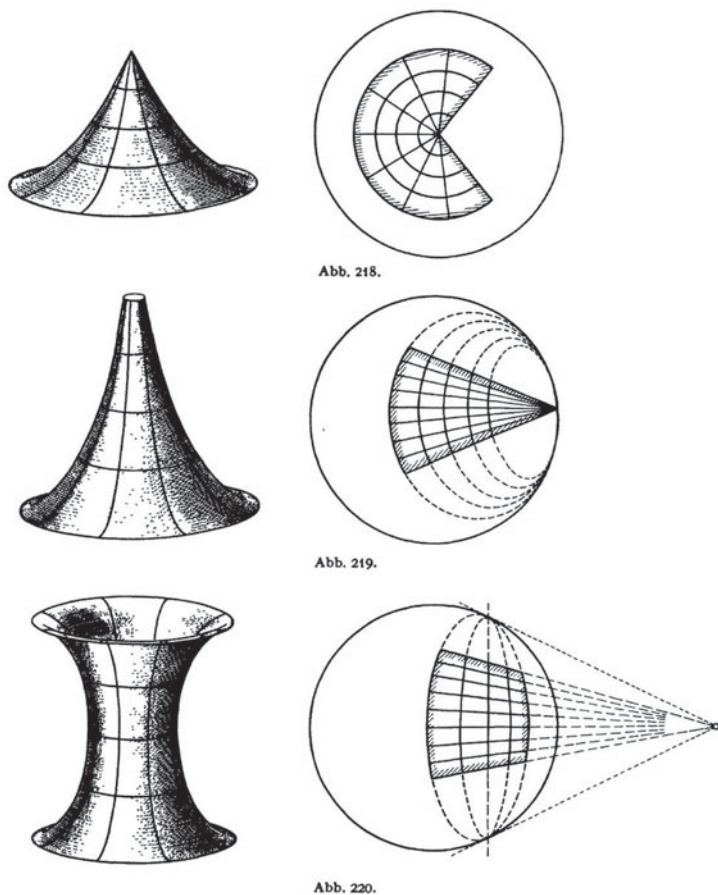


Figure 13.15: Geodesic-preserving mappings

All the axioms of Euclid, except the parallel axiom, hold in the new interpretation of “plane,” “line,” and “distance.” Instead of the parallel axiom, one has of course Axiom P_2 , since there is more than one “line” through a point P outside a given “line” L that does not meet L (Figure 13.16).

Beltrami also observed that the rigid motions of the “plane,” since they map lines to lines, are necessarily projective transformations. They are precisely those projective transformations of the plane that map the unit circle onto itself. Consequently, this model of the hyperbolic plane is often

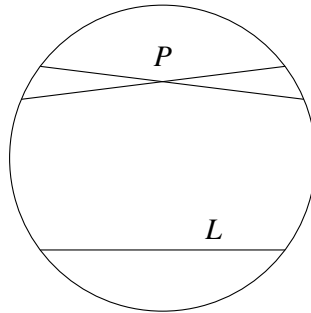


Figure 13.16: Failure of the parallel axiom

called the *projective model*. Cayley (1859) had already observed that these projective transformations could be used to define a “distance” $d(P, Q)$ in the unit disk—by saying $d(P, Q) = d(P', Q')$ if a transformation preserving the unit circle sends P to P' and Q to Q' —but he had not realized that the geometry obtained was that of Bolyai and Lobachevsky.

The pseudosphere is not entirely superseded by the projective model, since it remains the source of “real” distances and angles, whereas those in the projective model are necessarily distorted. One of the distinctive curves of the hyperbolic plane, the *horocycle*, or circle with center at infinity, is shown particularly clearly on the pseudosphere. If one imagines, following Beltrami (1868a), the pseudosphere wrapped by infinitely many turns of an infinitely thin covering, then the edge of this covering (along the rim of the pseudosphere) is a horocycle. The middle picture of Figure 13.15 shows the image of one turn of the covering, drawn solidly, and horocycles resulting from continued unwrapping are shown as dashed lines.

EXERCISES

Klein’s three pictures illustrate the three types of *rigid motion* of the hyperbolic plane.

1. *Rotation*, in which one point of the plane is fixed and all other points move in *hyperbolic circles* about it. (A hyperbolic circle is the locus of a point moving at constant “distance” from a fixed point.)
2. *Limit rotation*, in which a point at infinity is fixed and all points of the plane move in horocycles centered on the fixed point at infinity.
3. *Translation*, in which a “line” moves along itself and the other points of the plane move along its *equidistant curves*. (An equidistant curve is the locus of a point moving at constant “distance” from a “line.”)

- 13.7.1** Pick out *hyperbolic circles* and *equidistant curves* in the top and bottom pictures in Figure 13.15.
- 13.7.2** If the center of rotation in the top picture were not at the center of the disk, do you think the hyperbolic circles would be Euclidean circles?
- 13.7.3** Observe that equidistant curves at nonzero “distance” from the invariant “line” are *not* “lines” (necessarily so, in view of al-Haytham’s equivalent of axiom P_1 mentioned in Section 13.5). Does the translation move a point on an equidistant curve farther than a point on the invariant line?
- 13.7.4** Give an example of three points in the hyperbolic plane, not in a “line,” that do not lie on a hyperbolic circle. (If this problem proves difficult, try it again after reading the next section.)

13.8 Beltrami’s Conformal Models

The projective model of the hyperbolic plane distorts angles as well as lengths. One can see this with the asymptotic geodesics on the pseudosphere, which clearly tend to tangency at infinity yet are mapped onto lines meeting at a nonzero angle at the boundary of the unit disk (Figure 13.15). Beltrami (1868b) found that models with true angles—the so-called *conformal models*—can be obtained by sacrificing straightness of “lines.” His basic conformal model is not, in fact, part of the plane but part of a hemisphere. It is erected over the projective model and its “lines” are vertical sections of the hemisphere (hence semicircles) over the “lines” of the projective model (Figure 13.17). The “distance” between points on the hemisphere is defined to be the “distance” between the points beneath them in the projective model. Later we will see that “distance” on the hemisphere also has a simple direct definition.

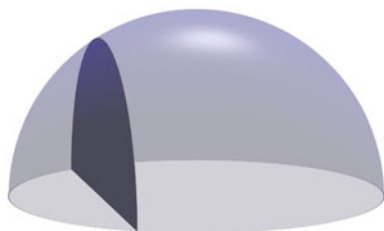


Figure 13.17: From the projective disk model to the hemisphere

The hemisphere model gives two planar conformal models by stereographic projection onto the tangent plane opposite the point of projection.

As we know from Section 12.2, stereographic projection preserves angles and sends circles to circles. The first model is a disk (Figure 13.18) that, by change of scale, can again be taken as the unit disk. (The lightbulb represents the point of projection, at the top of the sphere whose bottom hemisphere is shown.) The second (Figure 13.19) is a half-plane, which we take to be the upper half-plane, $y > 0$. Since the “lines” in the hemisphere model are circular and orthogonal to the equator, “lines” in the planar conformal models are again circular, orthogonal to the boundary of the disk and half-plane, respectively, or straight lines in exceptional cases. To avoid continual mention of these exceptional cases—namely, line segments through the disk center and lines $x = \text{constant}$ in the half-plane—we consider lines to be circles of infinite radius.

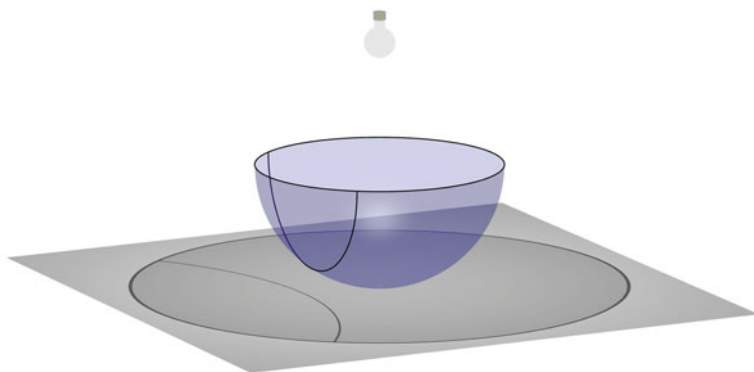


Figure 13.18: From the hemisphere to the conformal disk model

One of the beauties of the conformal models is that other important curves—hyperbolic “circles,” horocycles, and equidistant curves—are also real circles. Each curve equidistant from a given “line” L is a circle through the endpoints of L on the boundary. Horocycles are circles tangential to the boundary and also, in the half-plane model, the lines $y = \text{constant}$. A circle not meeting the boundary is a hyperbolic “circle,” but its “center,” at equal “distance” from all its points, is not at the Euclidean center. Figure 13.20 shows some of these curves. They are imprinted on a tessellation of the half-plane by triangles with angles $\pi/2$, $\pi/3$, and 0, called the *modular tessellation* because it depicts the periodicity of the modular function.

The triangles of the modular tessellation are bounded by “lines” and

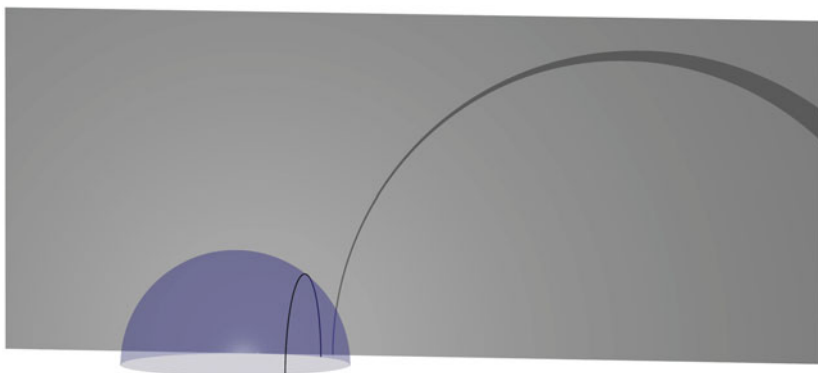


Figure 13.19: From the hemisphere to the half-plane model

they are in fact *congruent* in the sense of hyperbolic “distance.” This shows again that the boundary is infinitely far away, because there are infinitely many triangles below any point in the open half-plane. Note also that asymptotic “lines” are tangential at “infinity” (the boundary) and that the boundary is their common perpendicular, thus resolving the situation that Saccheri (Section 13.5) thought to be contradictory.

“Distance” is particularly easy to express in the half-plane model. The “distance” ds between neighboring points (x, y) and $(x + dx, y + dy)$ is

$$ds = \frac{\sqrt{dx^2 + dy^2}}{y},$$

that is, the Euclidean distance divided by y . Thus “distance” $\rightarrow \infty$ as a point approaches the boundary $y = 0$ of the half-plane, as expected. For constant x , integration along a vertical line shows that “distance” increases exponentially relative to Euclidean distance as y decreases. For example, when $x = 0$ and $y = 1, \frac{1}{2}, \frac{1}{4}, \dots$, the “distances” between successive points are equal. The formula for ds was first obtained by Liouville (1850) by directly mapping the pseudosphere into the half-plane. The “distance” formula for the conformal disk was also found before Beltrami, by Riemann (1854b), but neither Liouville nor Riemann saw the hyperbolic geometry.

Beltrami (1868b) not only found these models, in a unified way, but also extended the idea to n dimensions. For example, he gave a model of the three-dimensional space considered by Bolyai and Lobachevsky as the

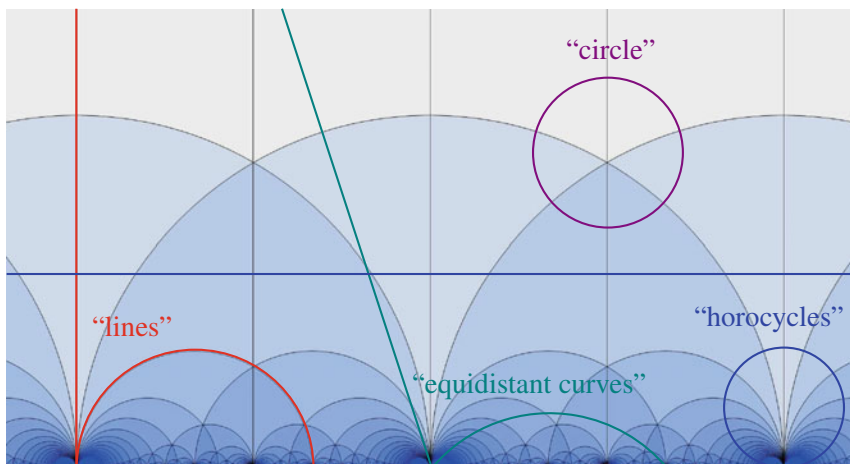


Figure 13.20: Some curves in the half-plane model

upper half, $z > 0$, of ordinary (x, y, z) -space, with “distance”

$$ds = \frac{\sqrt{dx^2 + dy^2 + dz^2}}{z}.$$

“Lines” are then semicircles orthogonal to $z = 0$ and “planes” are hemispheres orthogonal to $z = 0$. Restricting the “distance” function to such a hemisphere turns out to give Beltrami’s hemisphere model. Thus the hemisphere model can be viewed as a hyperbolic plane lying in hyperbolic 3-space. The horospheres of the half-space model are spheres tangential to $z = 0$, together with the planes $z = \text{constant}$. Beltrami (1868b) pointed out that on $z = \text{constant}$ we have

$$ds = \frac{\sqrt{dx^2 + dy^2 + dz^2}}{\text{constant}},$$

that is, “distance” is proportional to Euclidean distance. Thus he had an immediate proof of Wachter’s wonderful theorem that the geometry of the horosphere is Euclidean.

EXERCISES

The mapping of the pseudosphere into the half-plane may be carried out as follows, using the parametric equations for the tractrix found in Exercise 13.2.5:

$$x = \sigma - \tanh \sigma, \quad y = \operatorname{sech} \sigma.$$

First we replace the parameter σ by the arc length τ along the tractrix.

13.8.1 Show that $\tau = \int_0^\sigma \sqrt{1 + \left(\frac{dy}{dx}\right)^2} dx = \log \cosh \sigma$, and hence $y = e^{-\tau}$.

Now take τ and the angle X of rotation as the coordinates on the pseudosphere obtained by rotating the tractrix about the x -axis.

13.8.2 Show that the length subtended by angle dX on a circular cross section of the pseudosphere is

$$y dX = e^{-\tau} dX,$$

and hence the distance between nearby points (X, τ) and $(X + dX, \tau + d\tau)$ on the pseudosphere is given by

$$ds^2 = e^{-2\tau} dX^2 + d\tau^2.$$

13.8.3 Finally, introduce the variable $Y = e^\tau$ and conclude that $ds = \frac{\sqrt{dX^2 + dY^2}}{Y}$.

Thus the pseudosphere is mapped into the (X, Y) -plane with preservation of distance, provided distance in the (X, Y) plane is defined by

$$ds = \frac{\sqrt{dX^2 + dY^2}}{Y}.$$

It follows, from what was said above, that geodesics on the pseudosphere correspond to semicircles with centers on the X -axis. This throws some light on the problem raised in Section 13.4—describing geodesics on the pseudosphere.

13.8.4 Explain why the region of the (X, Y) -plane corresponding to the pseudosphere is bounded by $X = 0$ and $X = 2\pi$ and it lies above some $Y = \text{constant} > 0$.

13.8.5 By considering a semicircle crossing the region described in Exercise 13.8.4, show that there is no smooth closed geodesic on the pseudosphere.

13.9 The Complex Interpretations

One of the characteristics of the Euclidean plane is the existence of *regular tessellations*: tilings of the plane by regular polygons. There are three such tilings, based on the square, equilateral triangle, and regular hexagon (Figure 13.21).

Associated with each tiling is a *group of rigid motions* of the plane that maps the tiling pattern onto itself. For example, the unit square pattern is mapped onto itself by unit translations parallel to the x and y axes and by the rotation of $\pi/2$ about the origin, and these three motions generate all

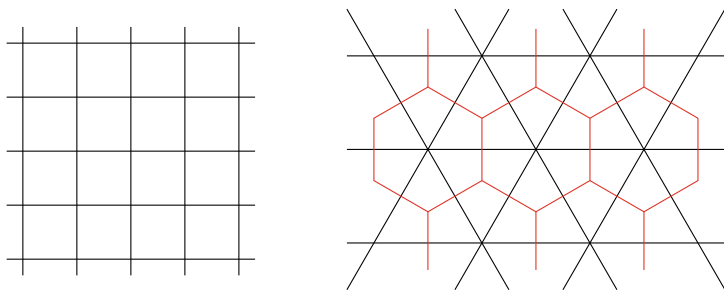


Figure 13.21: Tessellations of the Euclidean plane

motions of the tessellation onto itself. If we write $z = x + iy$, then these generating motions are given by the transformations

$$z \mapsto z + 1, \quad z \mapsto z + i, \quad z \mapsto zi.$$

The triangle and hexagon tessellations have a group generated by

$$z \mapsto z + 1, \quad z \mapsto z + \tau, \quad z \mapsto z\tau,$$

where $\tau = e^{i\pi/3}$ is the third vertex of the equilateral triangle whose other vertices are at 0, 1 (Figure 13.22). In fact, any motion of the Euclidean plane can be composed from translations $z \mapsto z + a$ and rotations $z \mapsto ze^{i\theta}$.

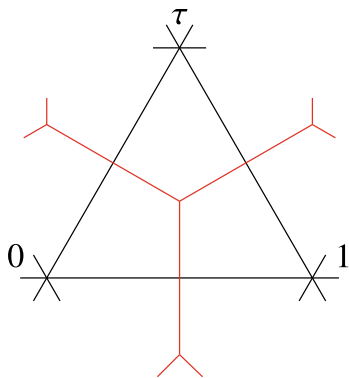


Figure 13.22: Relation between the triangle and hexagon tessellations

The sphere also has a finite number of regular tessellations, obtained by central projections of the regular polyhedra (Section 2.2). Figure 13.23 shows a tessellation corresponding to the icosahedron. (Each face has been further subdivided into six congruent triangles.) The motions mapping

such a tessellation onto itself can be expressed as complex transformations by interpreting the sphere as $\mathbb{C} \cup \{\infty\}$ via stereographic projection (Section 11.6). Gauss (1819) found that any motion of the sphere can be expressed by a transformation of the form

$$z \mapsto \frac{az + b}{-\bar{b}z + \bar{a}},$$

where $a, b \in \mathbb{C}$ and an overbar denotes the complex conjugate.

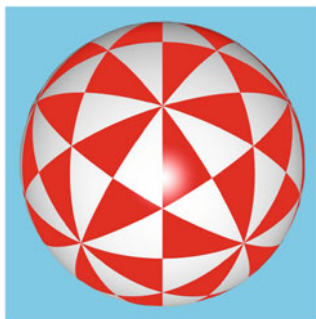


Figure 13.23: Icosahedral tessellation of the sphere

The conformal models of the hyperbolic plane can be regarded as parts of \mathbb{C} : the unit disk $\{z : |z| < 1\}$ and the half-plane $\{z : \text{Im}(z) > 0\}$. Their rigid motions, being conformal transformations, are complex functions, and Poincaré (1882) made the beautiful discovery that they are of the form

$$z \mapsto \frac{az + b}{\bar{b}z + \bar{a}} \quad \text{for the disk, and}$$

$$z \mapsto \frac{\alpha z + \beta}{\gamma z + \delta} \quad \text{for the half plane,}$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{R}$. Notice that the latter, with x in place of z , are the transformations of the projective line studied in Section 7.6. Thus the “line at infinity” of the hyperbolic plane is a projective line.

Infinitely many regular tessellations are possible, since the angles of a polygon can be made arbitrarily small by increasing its area. For example, there are tessellations by equilateral triangles in which n triangles meet at each vertex, for each $n \geq 7$, and similar variety occurs for other polygons (see exercises). Some of these tessellations were known *before* Poincaré

(1882) gave the complex interpretation of hyperbolic geometry, and even before models of hyperbolic geometry were known. Figure 13.24 shows a tessellation by equilateral triangles of angle $\pi/4$ found in unpublished, and unfortunately undated, work of Gauss (*Werke*, vol. VIII, p. 104).

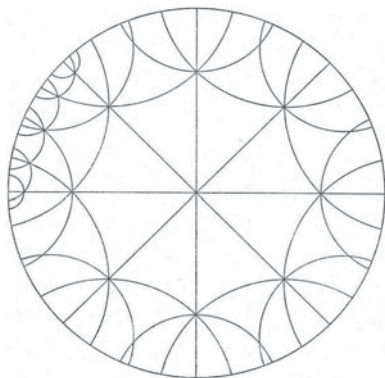


Figure 13.24: The Gauss tessellation

Others arise from differential equations and were discovered in this context by Riemann (1858b) and Schwarz (1872) (the first published example, Figure 13.25). By explaining these tessellations in terms of hyperbolic geometry, Poincaré (1882) showed that hyperbolic geometry was part of existing mathematics.

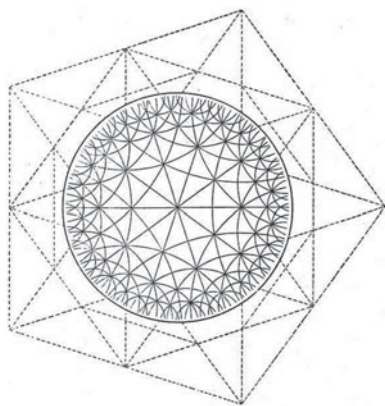


Figure 13.25: The Schwarz tessellation

In a subsequent paper, Poincaré (1883) explained the geometric nature

of *linear fractional transformations*,

$$z \mapsto \frac{az + b}{cz + d},$$

special cases of which, as we have just seen, express the rigid motions of the two-dimensional Euclidean, spherical, and hyperbolic geometries. He showed that each linear fractional transformation of the plane \mathbb{C} is induced by a hyperbolic motion of the three-dimensional half-space whose “plane at infinity” is \mathbb{C} ; thus Poincaré’s theorem embraces those of Wachter and Beltrami on the representation of two-dimensional Euclidean, spherical, and hyperbolic geometry within three-dimensional hyperbolic geometry.

EXERCISES

- 13.9.1** Show that a triangle in the hyperbolic plane can have any angle sum $< \pi$.
- 13.9.2** Deduce that there are equilateral triangles with angle $2\pi/n$ for each $n \geq 7$.
- 13.9.3** Also deduce that triangles with angle zero exist, in a certain sense, and that their area is finite.
- 13.9.4** Find corresponding results for regular n -gons.



14

Group Theory

PREVIEW

Group theory was the first branch of modern, or *abstract*, algebra to emerge from the old algebra of equations. Group theory today is often described as the theory of symmetry, and indeed groups have been inherent in symmetric objects since ancient times. However, extracting algebra from a symmetric object is a highly abstract exercise, and groups first appeared in situations where some algebra was already present.

One of the first nontrivial examples was the group of integers mod p , for prime p , used by Euler (1758) to prove Fermat's little theorem. Of course, Euler had no idea that he was using a group. But he did use one of the characteristic group properties, namely, the existence of inverses.

Likewise, Lagrange (1771) was not aware of the group concept when he studied permutations of the roots of equations. But he was using the group S_n of permutations of n things, and some of its subgroups.

It was Galois (1831a) who first truly grasped the group concept, and he used it brilliantly to explain what makes an equation solvable by radicals. In particular, he was able to explain why the general quintic equation is *not* solvable by radicals. These discoveries changed the face of algebra, though few mathematicians realized it at first.

In the second half of the 19th century the group concept spread from algebra to geometry, following the observation of Klein (1872) that each geometry is characterized by a *group of transformations*.

14.1 The Group Concept

The notion of group is one of the most important unifying ideas in mathematics. It draws together a wide range of mathematical structures for which a notion of combination, or “product,” exists. Such products include the ordinary arithmetical product of numbers, but a more typical example is the product, or composition, of functions. If f and g are functions, then fg is the function whose value for argument x is $f(g(x))$. (Thus fg means “apply g , then f .” We have to pay attention to order because in general $gf \neq fg$.)

A group G is defined formally to be a set with an operation, usually called *product* and denoted by juxtaposition, a specific element called the *identity* and written 1, and, for each $g \in G$, an element called the *inverse* of g and written g^{-1} , with the following properties:

- (i) $g_1(g_2g_3) = (g_1g_2)g_3$ for all $g_1, g_2, g_3 \in G$ (associative property)
- (ii) $g1 = 1g = g$ for all $g \in G$ (identity property)
- (iii) $gg^{-1} = g^{-1}g = 1$ for all $g \in G$ (inverse property)

These axioms emerged gradually in the course of experience with particular groups. The stories of some of these groups will be recounted below. In practice, properties (i) and (ii) are usually evident, and it is more important to ensure that the product operation is merely *defined* for all elements of G . Many mathematical concepts have been created in response to the desire, at first unconscious, for products to exist.

For example, we saw in Section 7.2 that a perspective view of a perspective view is not generally a perspective view. So if the “product” fg of perspective transformations f and g means the result of performing g then f , then fg does not always belong to the set of perspective transformations. The set of *projective* transformations is the smallest extension of the set of perspective transformations to a set on which the product is always defined, namely, the set of finite products of perspective transformations.

In other instances, concepts have arisen from the desire to have inverses. Negative numbers, for example, can be viewed as extending the set $\{0, 1, 2, 3, \dots\}$ of natural numbers to the set \mathbb{Z} of *integers*, in which each element has an inverse under the $+$ operation. (In cases like this one, where the group operation is naturally written as $+$, the identity element is written 0 and the inverse of g is written $-g$.) Another example is the extension

of the line \mathbb{R} to the real projective line $\mathbb{RP}^1 = \mathbb{R} \cup \{\infty\}$, which ensures that each linear fractional function has an inverse. Likewise, extending the plane by points at infinity ensures that each projective transformation has an inverse, because points projected to infinity can be projected back again.

Inverses sometimes appear unintentionally, as it were, in finite situations where repeated application of the group operation eventually produces the identity element. The simplest example is the *cyclic group* \mathbb{Z}_n , which consists of the numbers $0, 1, 2, \dots, n-1$ under addition modulo n , where numbers are called *congruent modulo n* when they differ by a multiple of n . Here the identity element is 0, and $n-1$ is the inverse of 1 because their sum is congruent to 0, modulo n . Similarly, $n-2$ is the inverse of 2, $n-3$ is the inverse of 3, and so on.

Perhaps the earliest nontrivial use of inverses occurs with multiplication modulo p , which Euler (1758) (and possibly Fermat before him) used to give an essentially group-theoretic proof of Fermat's little theorem. We proved this theorem with the help of the binomial theorem (and *without* using inverses) in Section 5.9. We now abbreviate “modulo” as “mod,” and assume p is prime.

Since integers m and n are congruent mod p if they differ by an integer multiple of p , b is an *inverse of a* under multiplication mod p if ab is congruent to 1 modulo p , that is, if $ab + kp = 1$ for some integer k . Since p is prime, such a b exists for each a not a multiple of p , by applying the Euclidean algorithm to the relatively prime numbers a, p (Section 3.3).

Euler did not define a group in his proof, but it is easy for us to do so (and to rephrase his proof accordingly; see exercises). The group elements are the numbers $1, 2, \dots, p-1$, and the product of a and b is defined to be $ab \bmod p$, where

$$ab \bmod p =$$

the number among $1, 2, \dots, p-1$ that is congruent to ab , mod p .

Group properties (i) and (ii) follow from ordinary arithmetic; (iii), as we have seen, follows from the Euclidean algorithm.

The preceding examples illustrate the influence of geometry and number theory on the group concept. An even more decisive influence was the theory of equations, which we look at briefly in Section 14.3. But first we need to understand a little about *subgroups*—the groups within a group—and when a subgroup may be said to “divide” a group. For a more detailed account of the development of the group concept, see Wussing (1984).

EXERCISES

A good introduction to inverses under multiplication mod p may be had with $p = 5$. There is no need to use the Euclidean algorithm to find these inverses—just multiply by numbers < 5 until a product congruent to 1 (mod 5) is obtained.

14.1.1 Find the inverses of 2, 3, and 4 under multiplication mod 5.

Now here is the proof of Fermat's little theorem using inverses mod p . Start with the nonzero numbers, mod p ,

$$1, \quad 2, \quad \dots, \quad (p-1),$$

and multiply them all by a nonzero a (mod p).

14.1.2 Notice that if we multiply again by the *inverse* of a (mod p) we get back the numbers

$$1, \quad 2, \quad \dots, \quad (p-1).$$

Why does this show that the numbers

$$a \cdot 1 \bmod p, \quad a \cdot 2 \bmod p, \quad \dots, \quad a(p-1) \bmod p$$

are distinct and nonzero?

14.1.3 Deduce from Exercise 14.1.2 that if a is nonzero (mod p), then

$$\{a \cdot 1 \bmod p, \quad a \cdot 2 \bmod p, \quad \dots, \quad a(p-1) \bmod p\}$$

is the same set as

$$\{1, \quad 2, \quad \dots, \quad (p-1)\}.$$

14.1.4 Deduce from Exercise 14.1.3 that

$$a^{p-1} \cdot 1 \cdot 2 \cdot \dots \cdot (p-1) \bmod p = 1 \cdot 2 \cdot \dots \cdot (p-1) \bmod p.$$

14.1.5 Finally, deduce that

$$a^{p-1} \bmod p = 1 \bmod p,$$

that is,

$$a^{p-1} \equiv 1 \pmod{p}$$

(Fermat's little theorem; the version in Section 5.9 results from multiplying each side by a).

14.2 Subgroups and Quotients

The group concept was implicit in mathematics for a long time before it became explicit. The first substantial theorem of the subject, now known as *Lagrange's theorem*, also came before the formalization of the group concept, but to state it we will take advantage of current terminology.

A subset H of a group G is called a *subgroup* of G if H is also a group (under the same operation that makes G a group). For example, the set \mathbb{Z} of integers is a subgroup of the group \mathbb{R} of real numbers, under the addition operation. Lagrange's theorem concerns the number of members of a group H , which we call the *order* of H and denote by $|H|$. It states that:

If H is a subgroup of a finite group G , then $|H|$ divides $|G|$.

Lagrange (1771) proved a special case. Jordan (1870) proved the general case and generously named the theorem after Lagrange. The proof depends on the notion of *coset*. For each g in G we have the *left coset* of H

$$gH = \{gh_1, gh_2, \dots, gh_k\}, \quad \text{where } H = \{h_1, h_2, \dots, h_k\}.$$

In words, gH is the set that results from multiplying each member of H on the left by g . (There are right cosets Hg defined similarly, but we do not need them for this proof.) The key properties of cosets are:

1. Each coset gH has $|H|$ members, because we can recover the members of H by multiplying each member of gH on the left by g^{-1} .
2. Any two different cosets g_1H and g_2H are disjoint. This is because, if g_1H and g_2H have a common member g , we have

$$g = g_1h_1 = g_2h_2 \quad \text{for some } h_1, h_2 \text{ in } H.$$

But then

$$g_1 = g_2h_2h_1^{-1} \quad (\text{multiplying on the right by } h_1^{-1}),$$

whence

$$g_1H = g_2(h_2h_1^{-1}H) = g_2H,$$

since $h_2h_1^{-1}$ is a member of H , and multiplying H by any one of its members gives back H .

It follows from these two properties that G can be split into disjoint sets gH , each of size $|H|$, so $|H|$ divides $|G|$. \square

Under certain conditions, it makes sense to *multiply* cosets by the rule

$$g_1H \cdot g_2H = g_1g_2H.$$

For this rule to make sense, we must get the same answer $g'_1g'_2H = g_1g_2H$ whenever $g'_1H = g_1H$ and $g'_2H = g_2H$. This happens when $gH = Hg$ for each g in G because, under this condition,

$$\begin{aligned} g'_1g'_2H &= g'_1Hg'_2 && \text{because } g'_2H = Hg'_2, \\ &= g_1Hg'_2 && \text{because } g_1H = g'_1H, \\ &= g_1g'_2H && \text{because } g'_2H = Hg'_2, \\ &= g_1g_2H && \text{because } g'_2H = g_2H. \end{aligned} \quad \square$$

We call H a *normal* subgroup of G if it satisfies the condition $gH = Hg$ for each g in G , and in this case the cosets form a *group* called G/H , the *quotient* of G by H . The group properties are inherited from G , as is easy to check (see exercises).

If G has the property that $gg' = g'g$ for all g, g' in G (in which case we call G *abelian*, for reasons that will be explained in the next section), then obviously $gH = Hg$ for any subgroup H . This means that any subgroup H of an abelian group G is normal, and we can form the quotient group G/H . The concept of normal subgroup is therefore interesting only when G is *not* an abelian group. In this case, the first step towards understanding the structure of G is to look for normal subgroups.

All this was first understood and made explicit by Galois, whose work we introduce in the next section.

EXERCISES

The group properties of G/H follow from the definition of the product of cosets, $g_1H \cdot g_2H = g_1g_2H$.

14.2.1 Show that

$$g_1H(g_2H \cdot g_3H) = (g_1H \cdot g_2H) \cdot g_3H \quad \text{if and only if} \quad g_1(g_2g_3) = (g_1g_2)g_3;$$

hence associativity in G/H follows from associativity in G .

14.2.2 Show that $H = 1H$ is the identity element of G/H .

14.2.3 What is the inverse of gH in G/H ? Explain your answer.

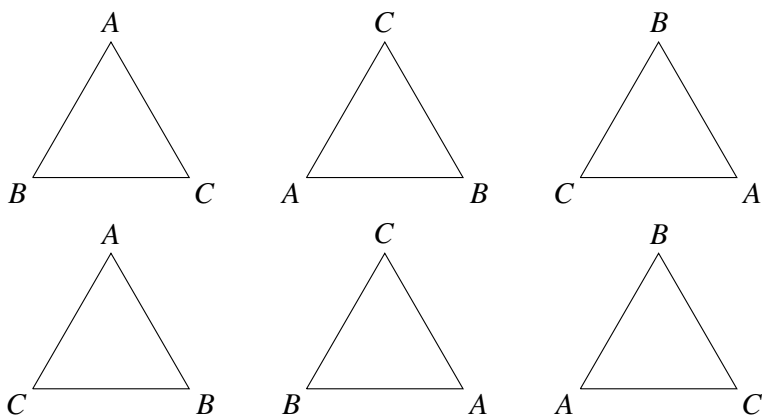


Figure 14.1: The symmetries of the equilateral triangle

The smallest nonabelian group is a group of six elements that may be viewed as the symmetries of the equilateral triangle. If we fix a position of the triangle, then there are six motions of it (including the “motion” that does not change it at all) leading to a position where it looks the same as it did before. These motions can be distinguished by where they send the vertices A , B , and C (Figure 14.1).

The six motions form a group (called S_3 for reasons that will be given in the next section) under the operation of combining motions. We combine motions by viewing each motion as a function $f(P)$ of points P in the triangle, so “do g , then f ” means to form the function $fg(P)$, as mentioned in Section 14.1.

- 14.2.4** Why are there only six motions leading to positions that look the same? Why is this group not abelian?
- 14.2.5** A subgroup H of S_3 consists of three rotations, through 0° , 120° , and 240° , represented by the pictures in the top row.
- 14.2.6** The bottom row of the picture represents a coset gH for some g in S_3 . Describe the motion g , and verify that Hg is the same set as gH .
- 14.2.7** Show that any subgroup H with only two cosets in a group G is a normal subgroup.

14.3 Permutations and Theory of Equations

We saw in Section 5.8 that, as early as 1321, Levi ben Gershon found that there are $n!$ permutations of n things. These permutations are invertible functions that form a group S_n (called the *symmetric group*) under

composition, though their behavior under composition was not considered until the 18th century. It was when the idea of permutation was applied to the roots of polynomial equations, by Vandermonde (1771) and Lagrange (1771), that the first truly group-theoretic properties of permutations came to light. At the same time, Vandermonde and Lagrange found the key to understanding the solution of equations by radicals.

They began with the observation that if an equation

$$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0 \quad (1)$$

has roots x_1, x_2, \dots, x_n , then

$$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = (x - x_1)(x - x_2) \cdots (x - x_n). \quad (2)$$

By multiplying out the right-hand side and comparing coefficients one finds that the a_i are certain functions of x_1, x_2, \dots, x_n . For example,

$$\begin{aligned} a_n &= (-1)^n x_1 x_2 \cdots x_n, \\ a_1 &= -(x_1 + x_2 + \cdots + x_n). \end{aligned}$$

These functions are *symmetric*, that is, unaltered by any permutation of x_1, x_2, \dots, x_n , since the right-hand side of (2) is unaltered by such permutations. Consequently, any rational function of a_1, a_2, \dots, a_n is symmetric as a function of x_1, x_2, \dots, x_n . Now the object of solution by radicals is to apply rational operations *and radicals* to a_1, a_2, \dots, a_n so as to obtain the roots—which are the completely *asymmetric* functions x_i .

Radicals must therefore reduce symmetry in some way, and one can see how in the quadratic case. The roots of

$$x^2 + a_1x + a_2 = (x - x_1)(x - x_2) = 0$$

are

$$x_1, x_2 = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2}}{2} = \frac{(x_1 + x_2) \pm \sqrt{x_1^2 - 2x_1x_2 + x_2^2}}{2},$$

and we notice that the symmetric functions $x_1 + x_2$ and $x_1^2 - 2x_1x_2 + x_2^2$ yield the two asymmetric functions x_1, x_2 when the two-valued radical $\sqrt{}$ is introduced. In general, a radical $\sqrt[p]{}$ multiplies the number of values of the function by p and divides symmetry by p , in the sense that the group

of permutations leaving the function unaltered is reduced to $1/p$ of its previous size.

Vandermonde and Lagrange found they could explain the previous solutions of cubic and quartic equations in terms of such symmetry reduction in the corresponding permutation groups, S_3 and S_4 . They also found some properties of subgroups, such as Lagrange's theorem mentioned in the previous section. However, they did not understand the relation between radicals and subgroups of S_n well enough to handle equations of degree ≥ 5 . Ruffini (1799) and Abel (1826) made enough progress with S_5 to be able to prove the unsolvability of the quintic, but they did not get beyond this. None of these authors were aware of the group concept, and it is only with hindsight that we can interpret their results in group-theoretic terms.

The concept, and indeed the word “group,” is due to Galois (1831b). Along with it, Galois introduced the concept of normal subgroup, which finally unlocks the secret of solvability by radicals. Galois showed that each equation E has a group G_E consisting of the permutations of the roots that leave rational functions of the coefficients unaltered, and that the reduction of symmetry caused by introduction of a radical corresponds to formation of a normal subgroup. More precisely, *if E is an equation solvable by radicals if and only if there is a chain of subgroups*

$$G_E = H_1 \supseteq H_2 \supseteq \cdots \supseteq H_k = \{1\}$$

such that each H_{i+1} is a normal subgroup of H_i and H_i/H_{i+1} is cyclic. (Moreover, if H_i/H_{i+1} is cyclic of order n then the step from H_i to H_{i+1} corresponds to introduction of an n th root.) Such a group G_E is now called *solvable* because it signals solvability of the corresponding equation.

Examples of solvable groups are S_3 and S_4 , as one would expect from the known solvability of the corresponding equations. Also, it is easy to see that all finite abelian groups are solvable, so each equation with an abelian group is solvable by radicals—a result due to Abel (1829). This is why we call such groups “abelian.” If E is the general equation of degree n , then $G_E = S_n$ and the theorem of Ruffini and Abel is recovered by showing that S_n is *not* solvable for $n \geq 5$ (see, for example, Dickson (1903)).

This brief sketch of Galois's ideas covers only a part of his theory. Another part is his theory of *fields*, which is needed to clarify the notion of rational function. We take up the theory of fields in Chapter . Group theory and field theory make up what is currently known as *Galois theory*

(see, for example, Edwards (1984)). What one might consider to be the summit of Galois's theory, the solution of equations by elliptic and related functions, is currently a fairly remote specialty. It appears in earlier books such as Jordan (1870) and Klein (1884), and more recently in McKean and Moll (1997). The greatest triumph of this theory was the solution of the general quintic equation by elliptic modular functions in Hermite (1858), following a hint in Galois (1831a) (see also Section 14.8).

EXERCISES

The simplest type of permutation is a *transposition*, which swaps two things and leaves the others fixed.

14.3.1 Show that any permutation is a product of transpositions, that is, any arrangement of n things may be achieved by repeated swaps.

The group S_n of all permutations of n things has an important subgroup A_n , consisting of the *even permutations*. An *even permutation* f of $\{1, 2, \dots, n\}$ is one with an even number of *inversions*, that is, pairs (i, j) for which $i < j$ and $f(i) > f(j)$ (Cramer (1750), p. 658).

Evenness can be seen by placing the numbers $1, 2, \dots, n$ in two rows, one above the other, and drawing a line from k in the top row to $f(k)$ in the bottom row. Figure 14.2 shows the permutation $f(1) = 2, f(2) = 3, f(3) = 1$ in this way.

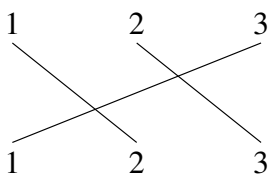


Figure 14.2: A permutation diagram

- 14.3.2** Explain why a permutation is even if and only if its diagram has an even number of crossings.
- 14.3.3** Show that the product of even permutations is even, so the even permutations of $\{1, 2, \dots, n\}$ form a group A_n . (It is called the *alternating group*.)
- 14.3.4** Show that evenness does not depend on how the numbers $1, 2, \dots, n$ are assigned to the n things. (Hint: if the numbers are permuted by g , show that the permutation f is replaced by the permutation $g^{-1}fg$.)
- 14.3.5** If g is an odd permutation, that is, $g \in S_n - A_n$, show that the set $gA_n = \{gf : f \in A_n\}$ is all the odd permutations in S_n ; hence A_n contains exactly half the members of S_n .

It follows from Exercise 14.3.5, and Exercise 14.2.7, that A_n is a normal subgroup of S_n ; hence we can always form the cyclic quotient $S_n/A_n = \mathbb{Z}_2$. Thus the real problem in solving the general equation of degree n is to “solve” A_n by finding normal subgroups inside it.

The group S_3 turns out to be solvable because its normal subgroup A_3 is already cyclic. This can be seen by studying the permutations in A_3 , but more easily by interpreting S_3 geometrically.

14.3.6 Interpret the symmetry group of the equilateral triangle, discussed in the previous exercise set, as the group S_3 of all permutations of three things.

14.3.7 Show that, under this interpretation, the cyclic subgroup of rotations is A_3 .

The interpretation we speak of here is an example of what is technically called an *isomorphism* between the triangle symmetry group and S_3 . An isomorphism is a one-to-one correspondence between the two groups that preserves the group operation, thus establishing that the groups have the “same form.” (We used this expression in the same sense in Section 12.5.) In calling the rotation subgroup cyclic we also imply an isomorphism, namely, the one that pairs the rotations through 0° , 120° , 240° with the members 0, 1, 2 of \mathbb{Z}_3 respectively.

14.3.8 Show that there is an isomorphism between the symmetry group of the regular tetrahedron and S_4 . To which symmetries do the members of A_4 correspond?

14.4 Permutation Groups

Galois understood “group” to mean a group of permutations of a finite set, so his definition stated only that the product of two permutations in the group must again be a member of the group. Associativity, identity, and inverses were consequences of his assumptions, and indeed too obvious to be considered important from his point of view. Galois’s work was published only in 1846, and by that time the theory of finite permutation groups had been taken up and systematized by Cauchy (1844). Cauchy likewise required only closure under product in his definition of group, but he recognized the importance of identity and inverses by introducing the notation of 1 for the identity and f^{-1} for the inverse of f .

Cayley (1854) was the first to consider the possibility of more abstract group elements, and with it the need to postulate associativity. (Incidentally, a group operation for which associativity is not obvious is that defined by the chord construction on a cubic curve: see Sections 10.3 and 12.5.) He took group elements to be simply “symbols,” with a “product” of A and B written $A \cdot B$ and subject to the law $A \cdot (B \cdot C) = (A \cdot B) \cdot C$, and a

unique element 1 subject to the laws $A \cdot 1 = 1 \cdot A = A$. He still assumed that each group was finite, however. This meant that the existence of inverses did not have to be postulated, only the validity of *cancellation*.

The existence of inverses in a finite group G , as defined by Cayley, follows from an argument used by Cauchy (1815) and developed more fully in Cauchy (1844). If $A \in G$, then the powers A^2, A^3, \dots all belong to G and hence they eventually include a recurrence of the same element:

$$A^m = A^n \quad \text{where } m < n.$$

Then, assuming that it is valid to cancel A^m from both sides, A^{n-m} is the identity element 1 and A^{n-m-1} is the inverse of A .

The need to postulate inverses first arises with infinite groups, where this argument no longer holds. Geometry was historically the most important source of infinite groups, as we will see in Section 14.6. It was in extending Cayley's abstract group theory to cover the symmetry groups of infinite tessellations that Dyck (1883) made the first mention of inverses in the definition of groups. We return to Dyck's concept of group in Section 14.7.

A theorem of Cayley (1878) shows that abstraction of the group concept is, in a sense, empty, because every group is essentially the same as a group of permutations. Cayley proved the theorem for finite groups only, where it is more valuable, but the proof easily extends to arbitrary groups (see exercises).

EXERCISES

The proof of Cayley's theorem goes as follows. Given any group G , associate any g in G with the function $\times g$ that sends each $h \in G$ to hg .

- 14.4.1** Show that function $\times g$ is a permutation of G , by showing that its effect can be undone by the function $\times g^{-1}$.
- 14.4.2** Show that different group elements g_1, g_2 give different functions $\times g_1, \times g_2$, and hence that there is a one-to-one correspondence between the elements g in G and the permutations $\times g$ of G .
- 14.4.3** Show that the permutation of G obtained by applying $\times g_1$, then $\times g_2$, is the permutation obtained by applying $\times g_1 g_2$.

Thus the group of permutations $\times g$ is *isomorphic* to the group G , in the sense described in the previous exercise set. This is the precise way of saying that G is essentially the same as a group of permutations.

14.5 Polyhedral Groups

A beautiful illustration of Cayley's theorem that every group is a permutation group is provided by the regular polyhedra, whose rotation groups turn out to be important subgroups of S_4 and S_5 . If we imagine a polyhedron P occupying a region R in space, the rotations of P can be viewed as the different ways of fitting P into R .

We begin with the rotations of the tetrahedron T . T has four vertices, V_1, V_2, V_3, V_4 , so each rotation of T is determined by a permutation of the four things V_1, V_2, V_3, V_4 . There are $4 \times 3 = 12$ rotations, because V_1 can be put at any of the four vertices of R , after which three choices remain for the remaining triangle of vertices V_2, V_3, V_4 . One can check, using the fact that a permutation that leaves one element fixed and rotates the other three is even, that all the symmetries of T are even permutations of V_1, V_2, V_3, V_4 . But the subgroup A_4 of *all* even permutations in S_4 has $\frac{1}{2} \times 4! = 12$ elements by the exercises in Section 14.3, so the rotation group of T is precisely A_4 .

The full permutation group S_4 can be realized by the rotations of the cube. The four elements of the cube that are permuted are the long diagonals (shown in red, yellow, blue, and green in Figure 14.3).

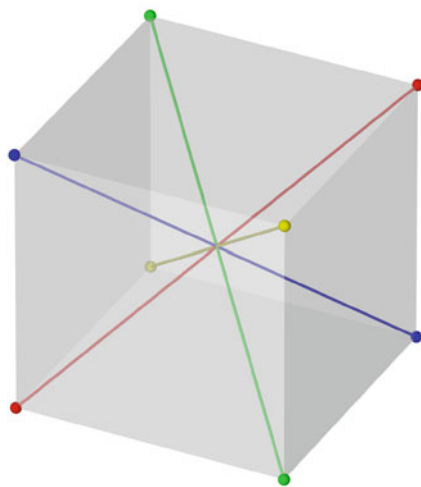


Figure 14.3: The cube and its diagonals

One has to check, first, that each permutation of the diagonals actually occurs. While doing this, it becomes apparent that the position of the diagonals (bearing in mind that endpoints could be swapped) really determines

the position of the cube (Exercise 14.5.1). S_4 is also the rotation group of the octahedron, because of the dual relationship between cube and octahedron seen in Figure 14.4. Each rotation of the cube is clearly a rotation of its dual octahedron, and conversely.

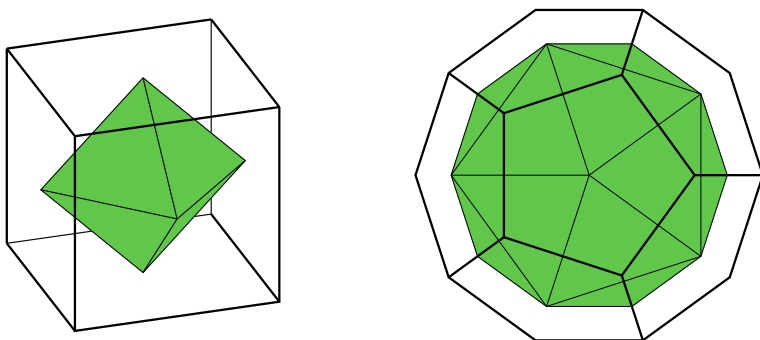


Figure 14.4: Dual polyhedra

Likewise, the dual relationship between dodecahedron and icosahedron (Figure 14.4) shows that they have the same rotation group. This group turns out to be A_5 , the subgroup of even permutations in S_5 . The five elements of the dodecahedron whose even permutations determine these rotations are tetrahedra formed from sets of four vertices (see Figure 14.5).



Figure 14.5: The tetrahedra in a dodecahedron

More on the polyhedral groups is in the famous book of Klein (1884), relating the theory of equations to the rotations of the regular polyhedra and functions of a complex variable. The complex variable makes its appearance when the regular polyhedra are replaced by regular tessellations of the sphere $\mathbb{C} \cup \{\infty\}$, and their rotations by linear fractional transformations, as in Section 13.9. Klein (1876) showed that, with trivial exceptions, *all* finite groups of linear fractional transformations come from the rotations of the regular polyhedra in this way.

The regular polyhedra were also the source of another approach to groups: *presentation by generators and relations*. Hamilton (1856) showed that the icosahedral group can be generated by three elements ι, χ, λ subject to the relations

$$\iota^2 = \chi^3 = \lambda^5 = 1, \quad \lambda = \iota\chi. \quad (1)$$

This means that any element of the icosahedral group is a product (possibly with repetitions) of ι, χ, λ and that any relation between ι, χ, λ follows from the relations (1). Dyck (1882) gave similar presentations of the cube and tetrahedron groups, and for the groups of certain finite tessellations, as part of the first general discussion of generators and relations. We return to this in Section 14.7.

EXERCISES

14.5.1 Show that each permutation of the diagonals of a cube is realizable, for example by showing that each transposition is realizable.

14.5.2 Show that a permutation of the diagonals uniquely determines the position of the cube.

Now consider the following rotations of the cube:

$\iota = 180^\circ$ rotation about a line through the midpoints of opposite edges,

$\chi = 120^\circ$ rotation about a diagonal.

These obviously satisfy $\iota^2 = \chi^3 = 1$.

14.5.3 Show that $\iota\chi = \lambda$, where

$\lambda = 90^\circ$ rotation about a line through the centers of opposite faces,

where the lines are, for example, the blue, red, and green ones shown in Figure 14.6 (these lines are fixed in space, not in the cube).

14.5.4 Deduce from Exercise 14.5.3 that $\iota^2 = \chi^3 = (\iota\chi)^4 = 1$ for the cube.

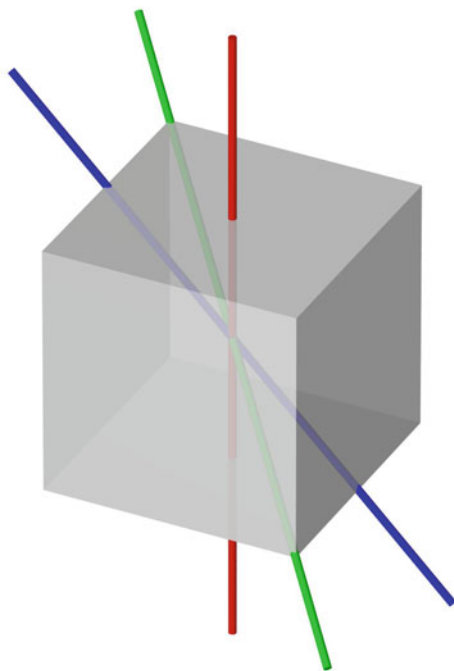


Figure 14.6: Rotation axes of the cube

14.5.5 Show that the analogous ι, χ for the tetrahedron satisfy

$$\iota^2 = \chi^3 = (\iota\chi)^3 = 1,$$

and the analogous ι, χ for the dodecahedron satisfy

$$\iota^2 = \chi^3 = (\iota\chi)^5 = 1.$$

14.6 Groups and Geometries

As the regular polyhedra show, geometric symmetry is fundamentally a group-theoretic notion. More generally, many notions of equivalence in geometry can be explained as properties preserved by certain groups of transformations. However, some revision of classical notions was needed before geometry could benefit from group-theoretic ideas.

The oldest notion of geometric equivalence is that of *congruence*. The Greeks understood figures F_1 and F_2 to be congruent if there is a rigid motion of F_1 that carries it into F_2 . But this concept of motion had meaning only for the individual figure. The “product” of motions of different figures was meaningless, so one did not have a group of motions.

The first step on the path to group theory in geometry was extending the idea of motion to the whole plane by Möbius (1827). This gave meaning to the product of motions. In fact, Möbius considered the class of all continuous transformations of the plane that preserve straightness of lines, and he picked out several subclasses: those that preserve length (congruences), shape (similarities), and parallelism (affinities). He showed that the most general continuous transformations preserving straightness are just the projective transformations, so in one stroke Möbius defined the notions of congruence, similarity, affinity, and projective equivalence as properties invariant under certain classes of transformations. That the classes in question are groups was obvious as soon as one recognized the concept of group. But the group concept was recognized only slowly: the ideas of Möbius were first stated in terms of groups by Klein (1872).

Klein's formulation became known as the *Erlanger Programm* because he announced it at the University of Erlangen. He associated each geometry with a group of transformations that preserve its characteristic properties. Thus, characteristic properties show up as *invariants of a group*. For example, the group of plane Euclidean geometry is the group of *Euclidean rigid motions*—transformations of \mathbb{R}^2 that preserve the Euclidean distance $\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$ between points (x_1, y_1) and (x_2, y_2) . Euclidean distance is therefore an invariant, by the very definition of the group.

A more interesting example is the group of the real projective line \mathbb{RP}^1 , studied in Section 7.6. Here we start with the group, the group of real linear fractional transformations, and *discover* its invariant, the cross-ratio, which is not at all obvious visually. Plane projective geometry is similarly associated with the group of projective transformations of \mathbb{RP}^2 , and its fundamental invariant is likewise the cross-ratio.

Plane hyperbolic geometry, in view of the projective model, can be defined by the group of projective transformations that map the unit circle onto itself. An important influence on the Erlanger Programm was indeed Cayley (1859), where this group was first shown to determine a geometry, and the subsequent realization of Klein (1871) that the elements of this group are the rigid motions of hyperbolic geometry. Not surprisingly, its fundamental invariant is the hyperbolic distance, and this turns out to be a function of the cross-ratio.

Poincaré (1882) discovered that the rigid motions of the half-plane model are determined by projective transformations of its boundary—the real projective line—as we saw in Section 13.9. So hyperbolic geome-

try is also definable by the group of real linear fractional transformations, by extending these transformations from the line to the half-plane. (For an introduction to hyperbolic geometry based on this idea, see Stillwell (2005).)

When geometry is reformulated in terms of groups, certain geometric questions become natural questions about groups. A regular tessellation, for example, corresponds to a subgroup of the full group of motions, consisting of those motions that map the tessellation onto itself. In the case of hyperbolic geometry, where the problem of classifying tessellations is formidable, the interplay between geometric and group-theoretic ideas proved to be very fruitful. In the work of Poincaré (1882, 1883) and Klein (1882b), group theory is the catalyst for a new synthesis of geometric, topological, and combinatorial ideas, which are described in Sections 14.7 and 15.5.

EXERCISES

If we view geometric objects (points, lines, curves, and so on) as subsets X of a space S , then relations such as congruence arise from groups of transformations of S in the following way. There is a group G of maps $g : S \rightarrow S$, and each geometric object X has a G -orbit $\{g(X) : g \in G\}$, consisting of the objects onto which X is mapped by elements of G .

For example, if Δ is a triangle in the plane \mathbb{R}^2 , and G consists of all transformations of \mathbb{R}^2 that preserve length, then $\{g(\Delta) : g \in G\}$ consists of all triangles congruent to Δ . This example shows that members of the same G -orbit are “equivalent” in a sense that depends on G . In fact, we always get an equivalence relation from a group in this way. Here is another example.

14.6.1 If $G = \{\text{similarities of } \mathbb{R}^2\}$, what is $\{g(\Delta) : g \in G\}$ for a triangle Δ ?

For any group G of transformations, we define a relation $X \cong_G Y$ (“ X is G -equivalent to Y ”) between subsets X, Y of S by

$$X \cong_G Y \Leftrightarrow X \text{ is in the } G\text{-orbit of } Y.$$

Then the group properties of G imply the following properties of the relation \cong_G .

14.6.2 Show that the relation \cong_G has the properties

$$\begin{array}{ll} X \cong_G X & \text{(reflexive)} \\ X \cong_G Y \Rightarrow Y \cong_G X & \text{(symmetric)} \\ X \cong_G Y \text{ and } Y \cong_G Z \Rightarrow X \cong_G Z & \text{(transitive)} \end{array}$$

14.6.3 At which points does your solution of Exercise 14.6.2 involve the existence of an identity, existence of inverses, and existence of products in G ?

The properties in Exercise 14.6.2 show that \cong_G is an *equivalence relation*, according to the definition in the exercises for Section 2.1. There it was also noted that the reflexive and transitive properties actually imply symmetry, provided that transitivity is stated in the manner of Euclid's Common Notion 1: "Things equivalent to the same thing are equivalent to each other."

14.6.4 Prove Common Notion 1 for \cong_G :

$$X \cong_G Y \text{ and } Z \cong_G Y \Rightarrow X \cong_G Z.$$

You will see that this proof involves inverses, which previously were needed only to prove symmetry. This confirms that Euclid's Common Notion 1 is in some sense a combination of both transitivity and symmetry.

Returning to a particular group and its invariants, here is an example of the way in which an invariant can throw light on its group.

14.6.5 Given three points A, B, C on \mathbb{RP}^1 , show that there is a unique fourth point x such that the cross-ratio

$$\frac{(C - A)(x - B)}{(C - B)(x - A)}$$

has a given value y .

14.6.6 Deduce from Exercise 14.6.5 that each linear fractional transformation of \mathbb{RP}^1 is determined by its values on any three points A, B, C .

14.7 Combinatorial Group Theory

As mentioned in Section 14.5, the groups of the regular polyhedra were the first to be defined in terms of generators and relations. With finite groups such as these, however, one is concerned mainly with the simplicity and elegance of a presentation; the question of *existence* does not arise. For any finite group G one can trivially obtain a finite set of generators (namely, *all* the elements g_1, \dots, g_n of G) and defining relations (namely, all equations $g_i g_j = g_k$ holding among the generators). Of course the same argument gives an infinite set of generators and defining relations for an infinite group, but this is also not interesting. The problem is to find *finite* sets of generators and defining relations for infinite groups where possible.

This problem was first solved for the symmetry groups of certain regular tessellations, and such examples were the basis of the first systematic study of generators and relations, by Klein's student Dyck. Dyck's papers (1882, 1883) laid the foundations of this approach to group theory, now

called *combinatorial* (and, more recently, *geometric*). For more technical information, as well as detailed history of the development of combinatorial group theory, see Chandler and Magnus (1982).

Figure 14.7 illustrates how generators and relations arise naturally from tessellations. This tessellation is based on the regular tessellation of the Euclidean plane by unit squares, but each square has been subdivided into black and white triangles to eliminate symmetries by rotation and reflection. The symmetries that remain are generated by

1. horizontal translation of length 1
2. vertical translation of length 1

These generators are subject to the obvious relation

$$ab = ba,$$

which implies that any element of the group can be written in the form $a^m b^n$. If $g = a^{m_1} b^{n_1}$ and $h = a^{m_2} b^{n_2}$, then $g = h$ only if $m_1 = m_2$ and $n_1 = n_2$, that is, only if $g = h$ is a *consequence* of the relation $ab = ba$. Thus all relations $g = h$ in the group follow from $ab = ba$, which means that the latter relation is a defining relation of the group.

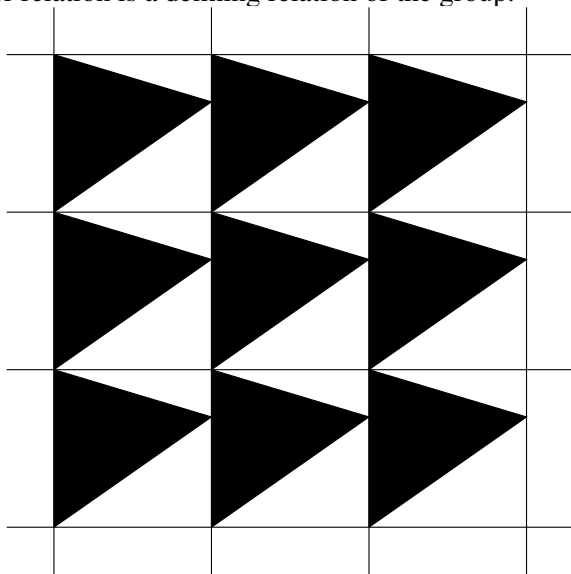


Figure 14.7: A tessellation of the plane

The obviousness of the defining relation in this case blinds us to a fact that becomes more evident with tessellations of the hyperbolic plane: *the generators and relations can be read off the tessellation*. Group elements correspond to cells in the tessellation, squares in the present example. If we fix the square corresponding to the identity element 1, then the square to which square 1 is sent by the group element g may be called square g . The generators $a^{\pm 1}$, $b^{\pm 1}$ are the elements that send square 1 to adjacent squares. They generate the group because square 1 can be sent to any other square by a series of moves from square to adjacent square. Relations correspond to equal sequences of moves or, what amounts to the same thing, to sequences of moves that return square 1 to its starting position. These sequences can all be derived from a circuit around a vertex (Figure 14.8), that is, the sequence $aba^{-1}b^{-1}$. Thus all relations are derived from $aba^{-1}b^{-1} = 1$, or, equivalently, $ab = ba$.

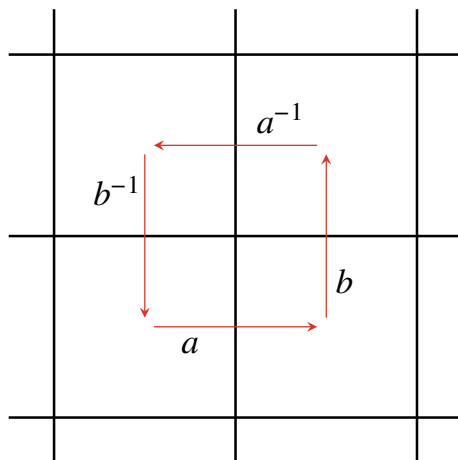


Figure 14.8: Circuit around a vertex

Generalizing these ideas, Poincaré (1882) showed that the symmetry groups of all regular tessellations, whether of the sphere, Euclidean plane, or hyperbolic plane, can be represented by finitely many generators and relations. Generators correspond to moves of the basic cell to adjacent cells, and hence to the sides of the basic cell; defining relations correspond to its circuits around its vertices. These results are also important for topology, as we will see in Chapter 15.

The notion of group abstracted from such examples was expressed in a somewhat technical way, involving normal subgroups, by Dyck (1882).

The following, simpler, approach was worked out by Dehn and used by Dehn's student Magnus (1930). A group G is defined by a set $\{a_1, a_2, \dots\}$ of *generators* and a set $\{W_1 = W'_1, W_2 = W'_2, \dots\}$ of *defining relations*. Each generator a_i is called a *letter*; a_i has an *inverse* a_i^{-1} , and arbitrary finite sequences ("products") of letters and inverse letters are called *words*.

Words W, W' are called *equivalent* if $W = W'$ is a consequence of the defining relations, that is, if W may be converted to W' by a sequence of replacements of subwords W_i by W'_i (or vice versa) and cancellation (or insertion) of subwords $a_i a_i^{-1}, a_i^{-1} a_i$. The elements of G are the equivalence classes

$$[W] = \{W' : W' \text{ is equivalent to } W\},$$

and the product of elements $[U], [V]$ is defined by

$$[U][V] = [UV],$$

where UV denotes the result of concatenating the words U, V . It has to be checked that this product is well defined, but once this is done, the group properties (i), (ii), and (iii) of Section 14.1 follow easily.

EXERCISES

Here is how one verifies that the classes $[W]$ have the group properties.

- 14.7.1** If U is equivalent to U' , show that UV is equivalent to $U'V$. Conclude, using this and a similar result for V' , that the product $[U][V]$ is independent of the choice of representatives for $[U], [V]$.
- 14.7.2** $[U]([V][W]) = ([U][V])[W]$ is trivial. Why?
- 14.7.3** Show that 1 = equivalence class of the empty word.
- 14.7.4** Show that $[W]^{-1} = [W^{-1}]$, where W^{-1} is the result of writing W backward and changing the sign of each exponent.

The smallest nonabelian group S_3 is also the smallest group with interesting defining relations. We take S_3 to be the group of symmetries of the equilateral triangle, as in the exercises to Section 14.2.

- 14.7.5** Show that S_3 is generated by a 120° rotation r about its center, and a 180° rotation s about the vertical axis of symmetry. Also show that r and s satisfy the relations

$$r^3 = s^2 = 1, \quad r^2 s = sr.$$

- 14.7.6** Deduce from Exercise 14.7.5 that each element of S_3 can be written in the form

$$r^m s^n, \quad \text{where } m = 0, 1, 2 \text{ and } n = 0, 1.$$

14.7.7 Conclude from Exercise 14.7.6 that $r^3 = s^2 = 1$ and $r^2s = sr$ are defining relations for S_3 .

14.7.8 By a similar argument, show the group of symmetries of a regular n -gon has defining relations $r^n = s^2 = 1$, $r^{n-1}s = sr$.

14.8 Finite Simple Groups

A group is called *simple* if it has no normal subgroups other than itself and the group $\{1\}$ whose only member is the identity element. The reason for the name is that a simple group cannot be “simplified” by forming the quotient G/H by a normal subgroup H . In this sense of simplicity, simple groups are like prime numbers, which cannot be “simplified” by dividing them by smaller integers. We do not claim that simple groups or prime numbers are not complicated!

The most obvious examples of finite simple groups *are* in fact the prime numbers, or more precisely the cyclic groups \mathbb{Z}_p for prime numbers p . \mathbb{Z}_p is simple because it has no subgroups whatever except itself and $\{1\}$ (thanks to Lagrange’s theorem that the size of a subgroup divides the size of the group). In fact, these are the only *abelian* simple groups, and we will ignore them from now on. The interesting simple groups are those that are not abelian, and the first examples were discovered by Galois in his study of polynomial equations.

The smallest nonabelian simple group is A_5 , the group of the 60 even permutations of five things. The simplicity of A_5 is the obstruction to the solution of the quintic equation by radicals. As we saw in Section 14.3, the group of the quintic equation is S_5 , the group of all 120 permutations of five things. Solving the quintic equation by radicals is equivalent to finding a chain of subgroups

$$S_5 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq \{1\}$$

such that the quotient of each group by the next is cyclic. We can make a first step,

$$S_5 \supseteq A_5,$$

but we can go no further because S_5 has no other nontrivial normal subgroup and A_5 is simple.

The proof that A_5 is simple (see exercises below) can be extended to show that A_n is simple for all $n \geq 5$, so Galois actually discovered a

whole infinite family of simple groups. He also found three remarkable simple groups in the study of *modular equations*, which arise in the theory of elliptic functions. The starting point of these investigations was the Fagnano (1718) formula for doubling the arc length of the lemniscate (Section 10.6):

$$2 \int_0^x \frac{dt}{\sqrt{1-t^4}} = \int_0^y \frac{dt}{\sqrt{1-t^4}}, \quad \text{where} \quad y = \frac{2x\sqrt{1-x^4}}{1+x^4}.$$

This gives the polynomial equation between x and y , of degree 2 in y :

$$y^2(1+x^4)^2 = 4x(1-x^4).$$

In the early 19th century, Fagnano's discovery was generalized to other elliptic integrals and to n -tupling instead of doubling, by Legendre, Gauss, Abel, and Jacobi. Galois left only some cryptic remarks about multiplication by 5, 7, and 11 (implying that they yield equations of degree 5, 7, and 11) in a letter that he wrote just before his death.

It turns out that the modular equation of degree 5 is equivalent to the general quintic equation, which is why Hermite (1858) was able to solve the general quintic equation by elliptic modular functions. However, the modular equations of degree 7 and 11 have groups of size 336 and 1320 respectively, so they are *not* symmetric groups S_n . The nature of these new groups was revealed by Jordan (1870). They can be viewed as (what we would now call) *transformation groups of finite projective lines*.

What is a finite projective line? It is like the real projective line $\mathbb{RP}^1 = \mathbb{R} \cup \{\infty\}$ discussed in Section 7.6, except that \mathbb{R} is replaced by a *finite field*. Finite fields were discovered by Galois, and we met some of them in Section 14.1 when we discussed addition and multiplication mod p . Since the latter operations have the same behavior as ordinary addition and multiplication—in particular, each nonzero number has an inverse—we can operate on the set $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ as we normally do, to solve equations and so on. Moreover, *linear fractional functions* make sense on $\mathbb{F}_p \cup \{\infty\}$, if we agree as usual that

$$1/0 = \infty \quad \text{and} \quad 1/\infty = 0.$$

So we can view $\mathbb{F}_p \cup \{\infty\}$ as a finite projective line, and its linear fractional functions as “projections.” Moreover, the cross-ratio makes sense on $\mathbb{F}_p \cup \{\infty\}$, and it is invariant under linear fractional functions by the same argument as in Section 7.6.

For this reason, the group of functions

$$x \mapsto \frac{ax+b}{cx+d}, \quad \text{where } a, b, c, d \in \mathbb{F}_p \quad \text{and} \quad ad - bc \neq 0,$$

is called the *projective general linear group*, $\text{PGL}(2, p)$. The reason for the 2 is that the coefficients a, b, c, d behave like the 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. It turns out that $\text{PGL}(2, 5)$, $\text{PGL}(2, 7)$, and $\text{PGL}(2, 11)$ are the groups of the modular equations of degree 5, 7, and 11 respectively. Moreover, each of these groups $\text{PGL}(2, p)$ contains a simple subgroup, called $\text{PSL}(2, p)$, which is half of its size. This was shown by Jordan (1870).

$\text{PSL}(2, 5)$ is the same as A_5 , but $\text{PSL}(2, 7)$ is a new simple group with 168 elements, and $\text{PSL}(11)$ is a simple group with 660 elements. It also happens that $\text{PSL}(2, 7)$ is the smallest nonabelian simple group, other than $\text{PSL}(2, 5) = A_5$. $\text{PSL}(2, 7)$ makes several other spectacular appearances in geometry, which may be seen in the article Gray (1982).

These examples give only the tiniest glimpse of the world of simple groups. Nevertheless, they hint at one of its most fascinating features—there are meaningful finite analogues of infinite structures such as the real projective line.

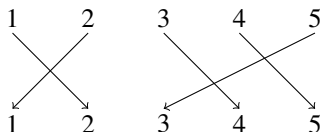
EXERCISES

A_5 is simple for quite elementary reasons, which can be understood with only slight knowledge of permutations. This includes the nature of even permutations, explored in the exercises to Section 14.3, and the decomposition of permutations into *cycles*, which we explore here.

We say that (a_1, a_2, \dots, a_k) is a *k-cycle* of a permutation f of $\{1, 2, \dots, n\}$ if

$$f(a_1) = a_2, \quad f(a_2) = a_3, \quad \dots, \quad f(a_k) = a_1$$

for distinct numbers a_1, a_2, \dots, a_k . Each number in $\{1, 2, \dots, n\}$ belongs to some *k-cycle* of f , so f is a product of disjoint cycles. For example, if f is



then $f = (1, 2)(3, 4, 5)$. It follows from the Exercises in Section 14.3 that the only even *k-cycles* among the even permutations of $\{1, 2, 3, 4, 5\}$ are the 3-cycles and the 5-cycles.

14.8.1 Omitting 1-cycles from the cycle decomposition, show that the only possible types of cycle decomposition for (nonidentity) members of A_5 are (a, b, c) , $(a, b)(c, d)$, and (a, b, c, d, e) .

14.8.2 Recalling that $f \cdot g$ means “ g , then f ,” check that

$$(i) \quad (1, 2, 3, 4, 5) \cdot (2, 1, 4, 3, 5) = (1, 5, 3).$$

$$(ii) \quad (1, 2)(3, 4) \cdot (1, 2)(4, 5) = (3, 4, 5).$$

The preceding exercises show that a subgroup H of A_5 with enough elements of type $(a, b)(c, d)$ or (a, b, c, d, e) also contains a 3-cycle. We now study what happens when H is normal and not equal to $\{1\}$, and show that such an H contains enough elements to ensure that 3-cycles are present.

Recall from Section 14.2 that a normal subgroup H of A_5 satisfies $gH = Hg$ for each g in A_5 . It follows that $gHg^{-1} = H$, that is, if h is in H , so is ghg^{-1} for any g in A_5 .

14.8.3 Show that if H contains a 5-cycle (a, b, c, d, e) then it also contains the 5-cycle $(g(a), g(b), g(c), g(d), g(e))$ for each g in A_5 .

14.8.4 Show that if H contains a product of 2-cycles $(a, b)(c, d)$ then it also contains the product of 2-cycles $(g(a), g(b))(g(c), g(d))$ for each g in A_5 .

14.8.5 Deduce from Exercises 14.8.3 and 14.8.4, and calculations like those in Exercise 14.8.2, that H contains a 3-cycle.

14.8.6 Deduce from the preceding exercises that H contains all 3-cycles.

To prove that A_5 is simple, it now remains to prove that the normal subgroup $H \neq \{1\}$ in fact contains all members of A_5 .

14.8.7 By using 3-cycles to produce other elements of A_5 , show that $H = A_5$.



15

Topology

PREVIEW

In Chapter 11 we saw how Riemann found the topological concept of *genus* to be important in the study of algebraic curves. In the present chapter we will see how topology became a major field of mathematics, with its own methods and problems.

Naturally, topology interacts with geometry, and it is common for topological ideas to be noticed first in geometry. An important example is the *Euler characteristic*, which was originally observed as a characteristic of polyhedra. Later it was seen to be meaningful for arbitrary closed surfaces. Today, we tend to think that topology comes first, and that it controls what can happen in geometry.

Topology also interacts with algebra. In this chapter we focus on the *fundamental group*, a group that describes the ways in which flexible loops can lie in a geometric object. On a sphere, all loops can be shrunk to a point, so the fundamental group is trivial. On the torus there are many nonshrinkable loops, but they are all combinations of two particular loops, a and b , where $ab = ba$. The latter relation is equivalent to $aba^{-1}b^{-1} = 1$, meaning that the product $aba^{-1}b^{-1}$ of loops is shrinkable to a point.

Thus the fundamental group presents itself naturally with *generators* (basic loops) and *relations* (shrinkable products of loops). This establishes a connection between topology and combinatorial group theory, discussed in Section 14.7. In fact, in a sense, topology contains *all* of combinatorial group theory. This is both a blessing and a curse: it allows group theory to be used in topology, but it infects topology with the hardest problems of combinatorial group theory.

15.1 Geometry and Topology

Topology deals with those properties that remain invariant under continuous transformations. In Klein's Erlanger Programm (where it is briefly mentioned under its old name of *analysis situs*) topology is the "geometry" of groups of continuous invertible transformations, or *homeomorphisms*. The "spaces" to which transformations apply, and indeed the meaning of "continuous," remain somewhat open. When these terms are interpreted in the most general way, as subject only to certain axioms (which do not concern us here), one has *general topology*. The theorems of general topology appear in fields ranging from set theory to analysis, but they are not very geometric in flavor. *Geometric topology*, the subject of this chapter, is obtained when the transformations are ordinary continuous functions on \mathbb{R}^n or on certain subsets of \mathbb{R}^n . Examples are the "topological equivalences" between surfaces we spoke about in Section 11.8.

Geometric topology is more recognizably "geometric" than general topology, though one would expect the "geometry" to be of a discrete and combinatorial kind. Ordinary geometric quantities—such as length, angle, and curvature—admit continuous variation and hence cannot be invariant under continuous transformations. Topologically invariant quantities are things such as the number of "pieces" of a figure or the number of "holes" in it. It turns out, though, that the discrete structures of topology are often reflected by discrete structures in ordinary geometry, such as polyhedra and tessellations. In surface topology, this geometric modeling of topological structure is so complete that topology becomes essentially a part of ordinary geometry. "Ordinary" here means geometry with notions of length, angle, and curvature—not necessarily Euclidean geometry. In fact, the natural geometric models of most surfaces are hyperbolic.

It remains to be seen whether topology as a whole will ever be subordinate to ordinary geometry. This is so in three dimensions, and here too hyperbolic geometry is the most important geometry (see Thurston (1997) or Weeks (1985)). In this chapter we make a virtue of a necessity by confining our discussion mainly to the topology of surfaces. This is the only area that is sufficiently understandable and relevant when set against the background of the rest of this book. Fortunately, this area is also rich enough to illustrate some important topological ideas, while still being mathematically tractable and visual. We begin the discussion of surface topology at its historical starting point, the theory of polyhedra.

15.2 Polyhedron Formulas of Descartes and Euler

The first topological property of polyhedra seems to have been discovered by Descartes around 1630. Descartes's short paper on the subject is lost, but its contents are known from a copy made by Leibniz in 1676, discovered among Leibniz's papers in 1860 and published in Prouhet (1860). A detailed study of this paper, including a translation and facsimile of the Leibniz manuscript, has been published by Federico (1982).

The same property was rediscovered by Euler (1752), and it is now known as the *Euler characteristic*. If a polyhedron has V vertices, E edges, and F faces, then its Euler characteristic is $V - E + F$. Euler showed that this quantity has certain invariance by showing

$$V - E + F = 2$$

for all convex polyhedra, a result now known as the *Euler polyhedron formula*. Descartes already had the same result implicitly in the pair of formulas

$$P = 2F + 2V - 4, \quad P = 2E,$$

where P is the number of what Descartes called “plane angles”: corners of faces determined by pairs of adjacent edges. The relation $P = 2E$ then follows from the observation that each edge participates in two corners. It should be stressed that Descartes's “plane angle” has nothing to do with angle measure, and hence is just as topological a concept as Euler's “edges.” Thus Descartes's result belongs to topology just as much as Euler's does, even though it fails to isolate the concept of Euler characteristic quite as well. Some rather hairsplitting distinctions have been made between Euler and Descartes in an effort to show that Euler invented topology and Descartes did not (see Federico (1982) for a review of different opinions).

Actually, neither of these mathematicians understood the polyhedron formula in a fully topological way. They both used nontopological concepts, such as angle measure, in their proofs, and they did not realize that “vertices,” “edges,” and “faces” are meaningful on any surface: edges need not be straight and faces need not be flat. Other early proofs of the Euler polyhedron formula also rely on angle measure and other ordinary geometric quantities. For example, that of Legendre (1794) assumes that the polyhedron can be projected onto the sphere, then uses the Harriot relation between angular excess and area for spherical polygons (Exercises 13.6.5, 15.2.1, and 15.2.2).

Probably the first to understand $V - E + F$ purely topologically was Poincaré (1895). In fact, Poincaré generalized the Euler characteristic to n -dimensional figures, but in the case of polyhedra his essential observation was this: a vertex divides an edge into two edges, and an edge divides a face into two faces. It follows that any subdivision of edges or faces of a polyhedron leaves $V - E + F$ unchanged: if a new vertex is introduced on an edge, V and E both increase by 1; if a new edge is introduced across a face, E and F both increase by 1. The reverse processes of amalgamation, where they make sense, likewise leave $V - E + F$ unchanged.

The constancy of $V - E + F$ over, say, the class of convex polyhedra then follows if it can be shown that any polyhedron P_1 in the class can be converted to any other, P_2 , by subdivisions and amalgamations. A plausible argument for this, due to Riemann (1851), is to view P_1 and P_2 as subdivisions of the same surface, say a sphere. Assuming that the edges of P_1 and P_2 meet only finitely often, superimposing P_1 on P_2 gives a common subdivision P_3 whose $V - E + F$ value is therefore the same as that of P_1 and P_2 . Hence the $V - E + F$ values of P_1 and P_2 are equal. A more general approach, which also yields the value of $V - E + F$ for *nonspherical* surfaces, is explained in the next section.

An engaging recent account of the Euler characteristic and its history is Richeson (2008).

EXERCISES

Here is the proof of the Euler polyhedron formula by Legendre (1794).

- 15.2.1** Consider the projection of a convex polyhedron onto a sphere, whose faces are therefore spherical polygons. Use the fact that

$$\text{area of a spherical } n\text{-gon} = \text{angle sum} - (n - 2)\pi$$

to conclude that

$$\text{total area} = 4\pi = \left(\sum \text{all angles}\right) - \pi\left(\sum \text{all } n\right) + 2\pi F.$$

- 15.2.2** Show also that

$$\sum \text{all } n = 2E, \quad \sum \text{all angles} = 2\pi V,$$

whence

$$V - E + F = 2.$$

The invariance of the Euler characteristic gives a simple topological proof that there are only five regular polyhedra. In fact, it shows that only five polyhedra

are *topologically regular* in the following sense: for some $m, n > 2$ their “faces” are topological m -gons on a topological sphere, n of which meet at each vertex. We show as follows that $V - E + F = 2$ allows only the pairs

$$(m, n) = (3, 3), (3, 4), (3, 5), (4, 3), (5, 3),$$

corresponding to the known regular polyhedra (Section 2.2).

15.2.3 Given that there are F faces, deduce that $E = mF/2$ and $V = mF/n$.

15.2.4 Apply the formula $V - E + F = 2$ to conclude that $4n/(2m + 2n - mn)$ is a positive integer.

15.2.5 Show that $2m + 2n - mn > 0$, that is, $2\frac{m}{n} + 2 > m$, only for the above pairs (m, n) .

15.2.6 Also check that $2m + 2n - mn$ divides $4n$ for these pairs.

15.3 The Classification of Surfaces

Between the 1850s and the 1880s, several different lines of research led to the demand for a topological classification of surfaces. One line, descending from Euler, was the classification of polyhedra. Another was the Riemann surface representation of algebraic curves, coming from Riemann (1851, 1857). Related to this was the problem of classifying symmetry groups of tessellations, considered by Poincaré (1882) and Klein (1882b) (see Section 15.4). Finally, there was the problem of classifying smooth closed surfaces in ordinary space (Möbius (1863)). These different lines of research converged when it was realized that each “surface” could be subdivided into “faces” by “edges” so as to become a generalized polyhedron. The generalized polyhedra were traditionally called *closed surfaces*, and are now described by topologists as *compact and without boundary*.

The subdivision argument for the invariance of the Euler characteristic $V - E + F$ applies to any such polyhedron, not just those homeomorphic to the sphere and not just those with straight edges and flat faces. Various mathematicians, such as Riemann (1851) and Jordan (1866), came to the conclusion that any closed surface is determined, up to homeomorphism, by its Euler characteristic. It also seemed that the different possible Euler characteristics were realized by the “normal form” surfaces seen in Figure 22.1, which were discovered by Möbius (1863). It is certainly plausible that these forms are distinct, topologically, because of their different numbers of “holes.” The main part of the proof is to show that any closed surface is homeomorphic to one of them.

The assumptions of Riemann (that the surface is a Riemann surface) and Möbius (that the surface is smoothly embedded in \mathbb{R}^3) were a little too special to yield a purely topological proof, and they also contained a hidden assumption of *orientability* (“two-sidedness”). A rigorous proof, from an axiomatic definition of generalized polyhedron, was given by Dehn and Heegaard (1907). The closed orientable surfaces indeed turn out to be those pictured in Figure 15.1, but in addition there are *nonorientable* surfaces, which are not homeomorphic to orientable surfaces.



Figure 15.1: Surfaces of genus 0, 1, 2, 3, ...

A nonorientable surface may be defined as one that contains a *Möbius band*, a nonclosed surface discovered independently by Möbius and Listing in 1858 (Figure 15.2).

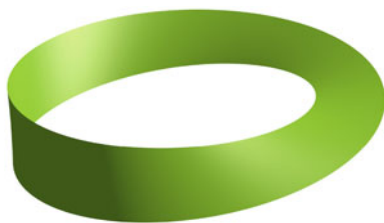


Figure 15.2: A Möbius band

Closed nonorientable surfaces cannot occur as Riemann surfaces, nor can they lie in \mathbb{R}^3 without crossing themselves; nevertheless, they include some important surfaces, such as the projective plane (Exercise 7.5.3). The nonorientable surfaces are also determined, up to homeomorphism, by the Euler characteristic.

The Möbius forms of closed orientable surfaces were given standard polyhedral structures by Klein (1882b). These are “minimal” subdivisions with just one face and, except for the sphere, with just one vertex. When the Klein subdivision of a surface is cut along its edges, one obtains a *fundamental polygon*, from which the surface may be reconstructed by pasting suitable edges. Figure 15.3 shows how to cut a torus, which can then be

flattened to a rectangle. (The process was shown in reverse in Figure 12.4.)



Figure 15.3: Cutting a torus

Figure 15.4 shows genus 2. The surface is cut open along a figure eight curve on the top, then further cut through each “handle.” The cut surface can then be spread out flat as an octagon whose eight corners are seen coming apart in the middle of the picture.

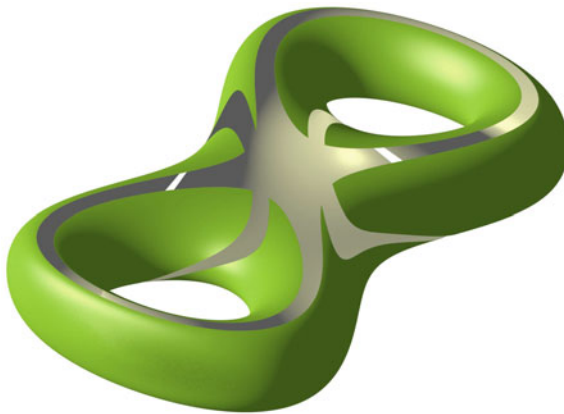


Figure 15.4: Cutting a genus 2 surface

It is often more convenient to work with the polygon rather than the surface or its polyhedral structure. For example, since Brahana (1921), most proofs of the classification theorem have used polygons rather than polyhedra, “cutting and pasting” them (instead of subdividing and amalgamating) until Klein’s fundamental polygons are obtained. The fundamental polygon gives a very easy calculation of the Euler characteristic χ and Exercise 15.3.1 shows it to be related to the *genus* g (number of “holes”) by

$$\chi = 2 - 2g.$$

EXERCISES

- 15.3.1** Show that the standard polyhedron for a surface of genus $g \geq 1$ has $V = 1$, $E = 2g$, $F = 1$, whence $\chi = 2 - 2g$.

The standard polygon for the genus g surface has a boundary path of the form $a_1 b_1 a_1^{-1} b_1^{-1} a_2 b_2 a_2^{-1} b_2^{-1} \cdots a_g b_g a_g^{-1} b_g^{-1}$, where successive letters denote successive edges and those with exponents -1 have oppositely directed arrows. Edges with the same letter are pasted together, with arrows matching.

- 15.3.2** Each sequence $a_i b_i a_i^{-1} b_i^{-1}$ is called a *handle*. Justify this term by drawing the surface that results from pasting together the matching edges of the polygon bounded by $a_i b_i a_i^{-1} b_i^{-1} c$. The result should be a “handle-shaped” surface with boundary curve c .

Another fundamental polygon is the “ $2n$ -gon with opposite edges pasted together,” that is, the polygon with boundary of the form $a_1 a_2 \cdots a_n a_1^{-1} a_2^{-1} \cdots a_n^{-1}$.

- 15.3.3** Show that for both $n = 2$ and $n = 3$ the surface obtained from the polygon $a_1 a_2 \cdots a_n a_1^{-1} a_2^{-1} \cdots a_n^{-1}$ is a torus.
- 15.3.4** Show that if n is even, the vertices of the polygon $a_1 a_2 \cdots a_n a_1^{-1} a_2^{-1} \cdots a_n^{-1}$ become a single vertex after pasting, and if n is odd they become two. Hence find the Euler characteristic of the surface for any n .

15.4 Surfaces and Planes

In Section 12.5 we noticed that an elliptic function maps a plane onto a torus. Such mappings are also interesting in the topological context, where they are called *universal coverings*. In general, a mapping $\varphi : \tilde{S} \rightarrow S$ of a surface \tilde{S} onto a surface S is called a *covering* if it is a homeomorphism locally, that is, when restricted to sufficiently small pieces of \tilde{S} . The mapping of the plane onto the torus in Section 12.5 is a covering because it is a homeomorphism when restricted to any region smaller than a period parallelogram.

Another example we already know is the mapping of the sphere onto the projective plane given by Klein (1874) (Section 7.5). This map sends each pair of antipodal points of the sphere to the same point of the projective plane, and hence is a homeomorphism when restricted to any part of the sphere smaller than a hemisphere. Yet another is Beltrami’s (1868a) covering of the pseudosphere by a horocyclic sector (Section 13.7). Topologically, this covering is the same as the covering of a half-cylinder by a half-plane when the plane is “wrapped” around the cylinder.

All these coverings are *universal* in the sense that the covering surface \tilde{S} (sphere or plane) can be covered only by \tilde{S} itself.

Since the sphere is covered only by itself, the interesting coverings of orientable surfaces are those for genus ≥ 1 (or Euler characteristic ≤ 0). All of these surfaces can be covered by planes. Moreover, each nonorientable surface can be doubly covered by an orientable surface in the same way that the projective plane is covered by the sphere, so the main thing to understand is the covering of orientable surfaces of genus ≥ 1 by planes.

The basic idea is due to Schwarz, and it became generally known through a letter from Klein (1882a) to Poincaré. To construct the universal covering of a surface S , take infinitely many copies of a fundamental polygon F for S and arrange them in the plane so that *adjacent* copies of F meet in the same way that F meets *itself* on S . For example, the torus T in Figure 15.5 has the rectangular fundamental polygon F shown, which meets itself along the red and blue edges in T (where the arrows indicate that edges must agree in direction as well as color).

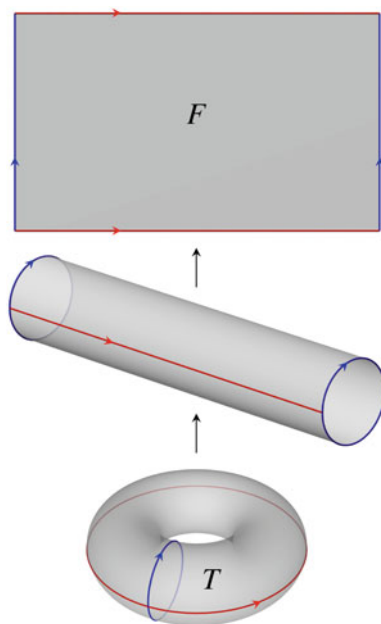


Figure 15.5: From the torus to its fundamental polygon

If instead we take infinitely many separate copies of F and join adjacent red and blue edges, then we obtain a plane \tilde{T} , tessellated as in Figure 15.6.

The universal covering $\tilde{T} \rightarrow T$ is then defined by mapping each copy of the rectangle F in \tilde{T} in the natural way onto the F in T .

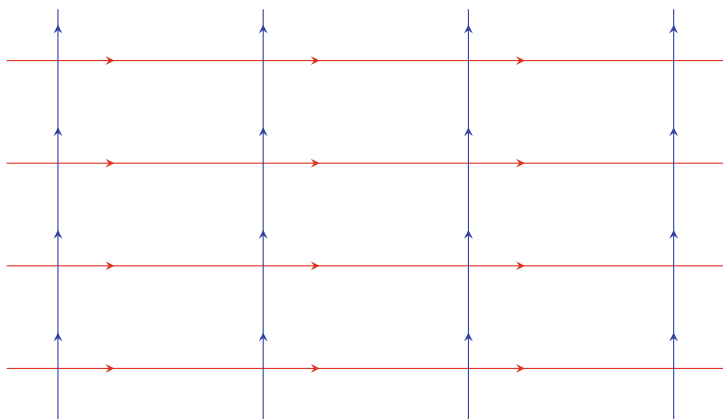


Figure 15.6: Tessellation of the torus cover

The tessellation of Figure 15.6 can of course be realized by rectangles in the Euclidean plane. We can therefore impose a Euclidean geometry on the torus by defining the distance between (sufficiently close) points on the torus to be the Euclidean distance between appropriate preimage points in the plane. In particular, the “straight lines” (geodesics) on the torus are the images of straight lines in the Euclidean plane. The torus geometry is not quite the geometry of the plane, of course, since there are closed geodesics, such as the images of the line segments a and b . However, it is Euclidean when restricted to sufficiently small regions. For example, the angle sum of each triangle on the torus is π .

For surfaces of genus >1 —that is, of negative Euler characteristic—the angle sum 2π of the fundamental polygon predicts negative curvature, and hence the natural covering plane should be hyperbolic. This can also be seen from the combinatorial nature of the tessellation on the universal cover. For example, the fundamental polygon F of the surface S of genus 2 is an octagon, as we saw in Figure 15.4.

In the universal covering, eight of these octagons have to meet at each vertex, since the eight corners of the single F meet on S . Such a tessellation is impossible, by regular octagons, in the Euclidean plane, but it exists in the hyperbolic plane, as Figure 15.7 shows.

In fact, this tessellation is obtained by amalgamating triangles in the Gauss tessellation (Figure 13.24). The tessellations for general genus >1

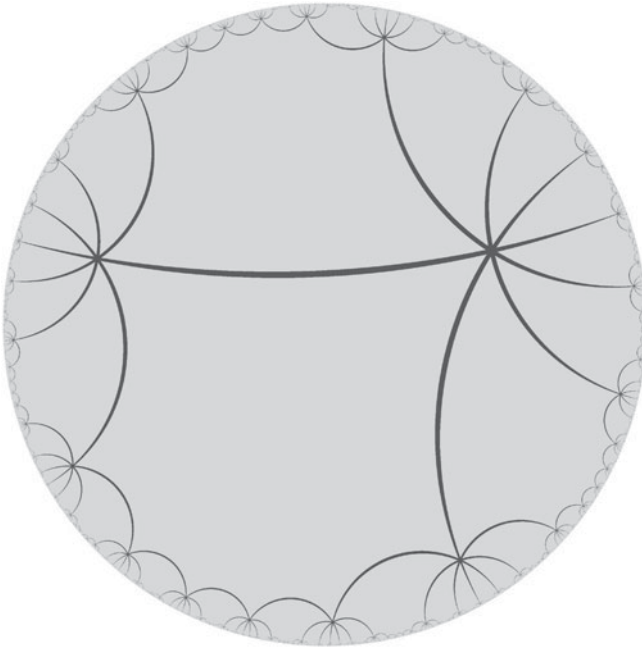


Figure 15.7: Tessellation of the genus-2 covering

can similarly be realized geometrically in the hyperbolic plane, and they were among the hyperbolic tessellations considered by Poincaré (1882) and Klein (1882b). The distance function, hence the curvature and local geometry, can be transported from the covering plane to the surface as we did above for the torus.

EXERCISES

When surfaces of genus >1 are realized as surfaces of constant negative curvature, their genus can be read off from their area.

- 15.4.1** Show that the fundamental polygon for an orientable surface of genus p is a $4p$ -gon with angle sum 2π .
- 15.4.2** Deduce that its Euler characteristic is proportional to its angular defect and hence to its area.
- 15.4.3** Conclude, using Exercise 15.3.1, that the area determines the genus.

15.5 The Fundamental Group

Another way to explore the meaning of the universal cover \tilde{S} is to use it to plot paths on the surface S . As a point P moves on S , each preimage \tilde{P} of P moves “above it” on \tilde{S} . This means in particular that as P crosses an edge of the fundamental polygon on S , \tilde{P} crosses from one polygon to its neighbor on \tilde{S} . So \tilde{P} will not necessarily return to its starting point, even when P does. In fact, the displacement of \tilde{P} measures the extent to which P winds around the surface S . Figure 15.8 shows an example. As P winds once around the torus from O , more or less in the direction of the red loop, \tilde{P} wanders from one end $\tilde{O}^{(1)}$ to the other $\tilde{O}^{(2)}$ of a red segment on \tilde{S} .

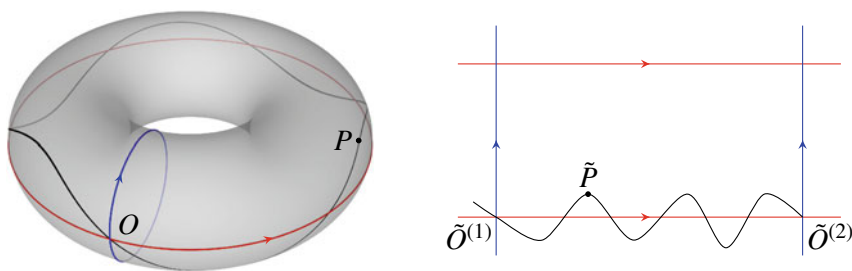


Figure 15.8: Plotting on the covering surface

We say that closed paths p, p' with initial point O on S “wind in the same way,” or are *homotopic*, if p can be deformed into p' with O fixed and without leaving the surface. Now if the path p of P is deformed into p' , with O fixed, then the path \tilde{p} of \tilde{P} is deformed into a \tilde{p}' with the same initial and final points, $\tilde{O}^{(1)}$ and $\tilde{O}^{(2)}$, as \tilde{p} . Hence each homotopy class corresponds simply to a *displacement* of the universal cover \tilde{S} that moves $\tilde{O}^{(1)}$ to $\tilde{O}^{(2)}$. The different preimages \tilde{P} will of course start at different preimages $\tilde{O}^{(1)}$ of O , but a single displacement of \tilde{S} moves them all to their final positions $\tilde{O}^{(2)}$. Moreover, the displacement moves the whole tessellation of \tilde{S} onto itself: it is a rigid motion of the tessellation.

Thus from the topological notion of homotopic closed paths we arrive back in ordinary geometry. We also arrive at a group called the *fundamental group* of S . Geometrically, it is the group of motions of \tilde{S} that map the tessellation onto itself (mapping each edge to an edge with the same color and direction). Topologically, it is the group of homotopy classes of closed paths, with a common initial point O , on S . The product of homotopy classes is defined by successive traversal of representative paths.

The fundamental group was first defined by Poincaré (1895). Poincaré defined it for much more general figures, whose universal covers are not so apparent, so he did not generally view the fundamental group as a covering motion group. However, Poincaré had already studied groups of motions of tessellations in his (1882), using linear fractional transformations. Reconsidering these earlier results topologically in his (1904), he arrived at the interpretation above. It includes, as we saw in Section 14.7, a presentation of the group by *generators* and *relations*. This discovery was very influential on the later work of Dehn (1912) and Nielsen (1927), which led ultimately to a recent surge of interest in hyperbolic geometry and geometric group theory. For some of these developments, see Serre (2003) and Clay and Margalit (2017).

The more general notion of fundamental group in Poincaré (1895) has also been influential outside topology. It turns out, for example, that for any “reasonably described” figure \mathcal{F} it is possible to compute generators and defining relations for the fundamental group of \mathcal{F} . The defining relations of a fundamental group can be quite arbitrary (in fact, *completely* arbitrary, as was shown by Dehn (1910) and Seifert and Threlfall (1934), p. 180). So the question arises: can the properties of a group be determined from its defining relations? One would like to know, for example, when two different sets of relations define the same group. The latter question was raised by Tietze (1908) in the first paper to follow up Poincaré’s work. Tietze made the remarkable conjecture—which could not even be precisely formulated at the time—that the problem is unsolvable. The *isomorphism problem for groups*, as it came to be known, was indeed shown to be unsolvable by Adyan (1957). Adyan’s result was based on the theory of algorithms, which will be outlined in Chapter 17.

By combining Adyan’s result with some of Tietze (1908) and the result of Seifert and Threlfall mentioned above, Markov (1958) was able to show the unsolvability of the *homeomorphism problem*. This is the problem of deciding, given “reasonably described” figures \mathcal{F}_1 and \mathcal{F}_2 , whether \mathcal{F}_1 is homeomorphic to \mathcal{F}_2 . The figures \mathcal{F}_1 and \mathcal{F}_2 can in fact be taken to be 4-dimensional “polyhedra.” (A complete proof of the unsolvability of the isomorphism problem and homeomorphism problem may be found in Stillwell (1993), and its history may be found in Stillwell (1982).) Thus Poincaré’s construction of the fundamental group led in the end to a quite unexpected conclusion: the basic problem of topology is unsolvable.

EXERCISES

In the following exercises it will be helpful to view the fundamental group as the group of motions of the universal covering plane, diagrammed in the previous section. The diagram shows that any sequence of motions equal to the identity corresponds to a closed path of edges in the diagram.

- 15.5.1** Explain why the fundamental group of the torus is generated by elements a and b with defining relation

$$aba^{-1}b^{-1} = 1.$$

- 15.5.2** Similarly, explain why the fundamental group of the surface of genus 2 is generated by elements a_1, b_1, a_2, b_2 with defining relation

$$a_1b_1a_1^{-1}b_1^{-1}a_2b_2a_2^{-1}b_2^{-1} = 1.$$

- 15.5.3** Show that the former group is commutative but the latter is not.



16

Commutative Algebra

PREVIEW

In modern algebra the first important concept to come to light was that of *groups*, as we have seen in Chapter 14. The distinctive feature of most groups, which sets them apart from traditional algebra, is *noncommutative multiplication*. In contrast, the key concepts of modern commutative algebra—*rings*, *fields*, and *vector spaces*—came to light only later, perhaps for the simple reason that at first they did not look different from traditional algebra.

Indeed, the concepts of ring and field are exemplified by the ancient concepts of integers and rational numbers. Their defining properties—the *axioms* for rings and fields—seem merely to encapsulate the common rules for calculation. It was noticed only in the 19th century that the ring and field properties are shared by systems quite different from the rational numbers, so experience *with* rational numbers can be used in other mathematical domains.

However, the domains that share the basic rules of calculation with integers and rational numbers may differ in other respects, especially in the nature of *primes*, where the very useful property of unique prime factorization may be lost. This raises the problem of generalizing the concept of prime, and finding conditions under which unique prime factorization may be regained.

This problem, uncovered by Kummer in 1844, spurred much of the development of commutative algebra in the 19th and early 20th centuries. It is this development—called *algebraic number theory*—that we follow in the later sections of this chapter.

16.1 Linear Algebra

Linear algebra began with the problem of solving sets of linear equations in several unknowns, which was solved by Chinese mathematicians about 2000 years ago by the method we now call Gaussian elimination. As mentioned in Section 5.2, the Chinese had a tool called the “counting board” that was ideal for such calculations, since it displayed the coefficients of the system in a square array, which could be operated upon just as we operate on matrices.

A harder problem is finding a *formula* that expresses the solution of a system

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &= b_n \end{aligned}$$

as a *function* of the coefficients a_{ij} and b_i . The solution is given by the rule

$$x_i = \frac{\det A_i}{\det A},$$

where $\det A$ is the *determinant* of the matrix

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

and A_i is the matrix obtained from A by replacing its i th column by the column of values b_j .

This rule is commonly called *Cramer’s rule* because of its appearance in the book Cramer (1750). However, it was known earlier. In a remarkable instance of independent discovery, Leibniz and the Japanese mathematician Seki discovered determinants around 1680, and independently developed their properties over the next few decades. Knobloch (2013) reveals the extent of Leibniz’s results on determinants, which were not published in his lifetime. Determinants also underlie the elimination process for polynomial equations, special cases of which were discovered by the Chinese, as we mentioned in Section 5.2.

Determinants were rediscovered several times, and they became the subject of a substantial theory in the 19th century. As late as 1960, determinants were considered important enough to be the subject of the four-volume history, Muir (1960). Their theory, well into the 20th century, completely overshadowed what we now call “linear algebra”; namely, the theory of vector spaces.

In this chapter we will assume (as we already have in some earlier chapters) that the reader knows the basic rules for calculating determinants. The only theoretical property of determinants we require is that linear homogeneous equations have a nonzero solution only if their determinant is zero. (This follows, for example, from Cramer’s rule and the property that a determinant with a zero column is zero.) As for vector spaces, we will develop their theory from scratch, because it is a simple but good example of modern algebraic thinking.

16.2 Vector Spaces

Grassmann (1844) introduced a very general, and sophisticated, theory of vector spaces, with inner and outer products. Because the idea was so new and, alas, very poorly explained by Grassmann, it was not understood by his contemporaries and went virtually unnoticed. Three years later, in an essay competition on the subject of Leibniz’s ideas about symbolic geometry, Grassmann (1847) made a second attempt. This time he emphasized the inner product as an encapsulation of the Pythagorean theorem, which makes a vector space “Euclidean.” Although Grassmann’s essay won the prize, his ideas did not really catch on until Peano formalized the concept of vector space (with due credit to Grassmann) in the 1880s.

The vector space axioms concern objects called *vectors*, denoted by $\mathbf{u}, \mathbf{v}, \mathbf{w}, \dots$ which can be added and multiplied by numbers a, b, c, \dots , called *scalars* in this context. The vectors include a *zero vector* $\mathbf{0}$ and, for each vector \mathbf{u} , its *negative* $-\mathbf{u}$. Then the axioms are, first, axioms for addition:

$$\begin{aligned}\mathbf{u} + \mathbf{v} &= \mathbf{v} + \mathbf{u}, \\ \mathbf{u} + (\mathbf{v} + \mathbf{w}) &= (\mathbf{u} + \mathbf{v}) + \mathbf{w}, \\ \mathbf{u} + \mathbf{0} &= \mathbf{u}, \\ \mathbf{u} + (-\mathbf{u}) &= \mathbf{0}.\end{aligned}$$

Then the following axioms for multiplication by scalars:

$$\begin{aligned} a(b\mathbf{u}) &= (ab)\mathbf{u}, \\ 1\mathbf{u} &= \mathbf{u}, \\ a(\mathbf{u} + \mathbf{v}) &= a\mathbf{u} + a\mathbf{v}, \\ (a + b)\mathbf{u} &= a\mathbf{u} + b\mathbf{u}. \end{aligned}$$

Since a, b, c, \dots are assumed to be real, these axioms of Peano are properly called axioms for a *real vector space*.

Grassmann developed his theory with the aim of algebraically creating a form of geometry, like Euclid's but without restriction to two or three dimensions. The concept of *dimension* of a vector space V arises from the concept of *basis*, which formalizes the idea of coordinates in V . A set of vectors $\mathbf{i}_1, \mathbf{i}_2, \dots, \mathbf{i}_n$ form a *basis of* V if:

- Each $\mathbf{u} \in V$ can be written in the form

$$\mathbf{u} = u_1\mathbf{i}_1 + u_2\mathbf{i}_2 + \cdots + u_n\mathbf{i}_n \quad \text{for some } u_1, u_2, \dots, u_n \in \mathbb{R},$$

in which case we say that $\mathbf{i}_1, \mathbf{i}_2, \dots, \mathbf{i}_n$ *span* V .

- A vector of the form

$$a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + \cdots + a_n\mathbf{i}_n \quad \text{for } a_1, a_2, \dots, a_n \in \mathbb{R},$$

equals $\mathbf{0}$ only if $a_1 = a_2 = \cdots = a_n = 0$, in which case we say that $\mathbf{i}_1, \mathbf{i}_2, \dots, \mathbf{i}_n$ are *linearly independent*.

It follows from these conditions that each vector \mathbf{u} is *uniquely* expressible in the form $u_1\mathbf{i}_1 + u_2\mathbf{i}_2 + \cdots + u_n\mathbf{i}_n$, so u_1, u_2, \dots, u_n serve as coordinates of \mathbf{u} with respect to the basis $\mathbf{i}_1, \mathbf{i}_2, \dots, \mathbf{i}_n$. Grassmann proved that any two bases of the same vector space V (assumed to have finite basis) are of the same size, n , called the *dimension* of V .

Any real vector space of dimension n is essentially the same as the space \mathbb{R}^n of ordered n -tuples $\mathbf{u} = \langle u_1, u_2, \dots, u_n \rangle$, where u_1, u_2, \dots, u_n are real numbers called the *components* of \mathbf{u} . In this realization, vectors are added to each other, and multiplied by numbers, componentwise:

$$\begin{aligned} \langle u_1, u_2, \dots, u_n \rangle + \langle v_1, v_2, \dots, v_n \rangle &= \langle u_1 + v_1, u_2 + v_2, \dots, u_n + v_n \rangle, \\ a\langle u_1, u_2, \dots, u_n \rangle &= \langle au_1, au_2, \dots, au_n \rangle. \end{aligned}$$

The *inner product* $\mathbf{u} \cdot \mathbf{v}$ of vectors

$$\mathbf{u} = \langle u_1, u_2, \dots, u_n \rangle \quad \text{and} \quad \mathbf{v} = \langle v_1, v_2, \dots, v_n \rangle$$

is defined by

$$\mathbf{u} \cdot \mathbf{v} = u_1 v_1 + u_2 v_2 + \dots + u_n v_n.$$

The inner product captures the concept of *length* of a vector (given by the Pythagorean theorem, first for $n = 2$, then inductively for larger n)

$$|\mathbf{u}| = \sqrt{u_1^2 + u_2^2 + \dots + u_n^2},$$

because

$$\mathbf{u} \cdot \mathbf{u} = u_1^2 + u_2^2 + \dots + u_n^2 = |\mathbf{u}|^2.$$

The inner product also captures the concept of angle because (less obviously)

$$\mathbf{u} \cdot \mathbf{v} = |\mathbf{u}||\mathbf{v}| \cos \theta,$$

where θ is the angle between the lines from $\mathbf{0}$ to the points \mathbf{u} and \mathbf{v} respectively. In particular, these lines are perpendicular when $\mathbf{u} \cdot \mathbf{v} = 0$. Because of this, many classical theorems about right angles have very slick proofs using the inner product (see exercises below).

By the early 20th-century, Klein was ready to include a smattering of Grassmann's ideas in the geometry volume, Klein (1909), of his *Elementary Mathematics From an Advanced Standpoint*. However, by this time algebraists had already extended the concept of vector space in a different direction. They observed that the fundamental properties of vector spaces, such as basis and dimension, do not require the scalars a, b, c, \dots to be real numbers. The same ideas apply as long as the scalars form a *field*.

EXERCISES

The invariance of basis size, which leads to the concept of dimension, was proved by Grassmann using the following lemma: *if n vectors $\mathbf{u}_1, \dots, \mathbf{u}_n$ span a vector space V over a field \mathbb{F} , then no $n+1$ vectors $\mathbf{v}_1, \dots, \mathbf{v}_{n+1}$ are independent*. Supposing the contrary, the proof is by a process of exchanging vectors \mathbf{u}_i by \mathbf{v}_j , one at a time, until all the \mathbf{u}_i are replaced. (The lemma is often called the “Steinitz exchange lemma,” though it is actually due to Grassmann.)

16.2.1 Suppose we have replaced $m-1$ of the \mathbf{u}_i by $\mathbf{v}_1, \dots, \mathbf{v}_{m-1}$, so that $\mathbf{v}_1, \dots, \mathbf{v}_{m-1}$ and the remaining \mathbf{u}_i span V . In particular,

$$\mathbf{v}_m = a_1 \mathbf{v}_1 + \dots + a_{m-1} \mathbf{v}_{m-1} + \text{terms } b_i \mathbf{u}_i \quad \text{where the } a_j, b_i \in \mathbb{F}.$$

Deduce that some $b_k \neq 0$, and hence that \mathbf{u}_k can be replaced by \mathbf{v}_m in the spanning set.

16.2.2 Conclude that v_1, \dots, v_n are also a spanning set, and show that this contradicts the linear independence of v_1, \dots, v_{n+1} .

A nice theorem that falls out of an inner product calculation is *concurrency of altitudes of a triangle*. An *altitude* is the line through a vertex of a triangle perpendicular to the opposite side. Figure 16.1 shows, in an example, that the three altitudes have a common point. To prove this in general we let vertices of the triangle be u, v, w , and choose the zero vector 0 to lie at the intersection of the altitudes of u and v .

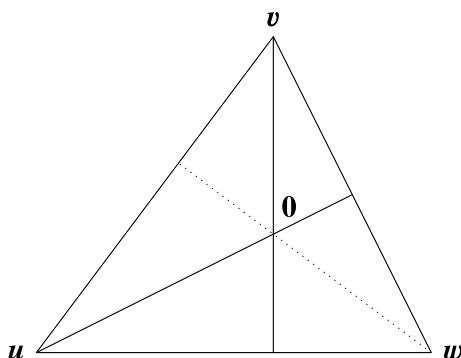


Figure 16.1: Altitudes of a triangle

16.2.3 Deduce from this choice of origin that $u \cdot (w - v) = 0$ and $v \cdot (u - w) = 0$.

16.2.4 Deduce in turn that $w \cdot (v - u) = 0$, so that the altitude through w also passes through 0 .

16.3 Fields

A *field* is a collection of objects that are added, subtracted, multiplied, and divided according to the rules of traditional algebra. These rules are now known as the *field axioms*:

$a + b = b + a$	$ab = ba$	(commutative laws)
$a + (b + c) = (a + b) + c$	$a(bc) = (ab)c$	(associative laws)
$a + (-a) = 0$	$a \cdot a^{-1} = 1$ for $a \neq 0$	(inverse laws)
$a + 0 = 0$	$a \cdot 1 = a$	(identity laws)
$a(b + c) = ab + ac$		(distributive law)

Thus it could be said that fields were the subject of *all* algebra up to the 19th century. Up to that time, the “laws of algebra” went without saying, as did the subject of those laws.

In retrospect, we can say that the pre-modern algebraists actually worked with several different fields:

- In basic arithmetic, the field \mathbb{Q} of rational numbers.
- In more sophisticated arithmetic, where roots and logarithms are present, the field \mathbb{R} of real numbers (though real numbers were not yet precisely defined).
- In solving polynomial equations, the field \mathbb{C} of complex numbers.
- In the “Universal Arithmetic” of symbolic calculation in “unknowns” x, y, z, \dots one had fields of *rational functions* in several variables.

The concept of field gradually came to light in the 19th century, when several new, and radically different, fields came to light:

- *Finite fields*, discovered by Galois in the 1820s. They include the field \mathbb{F}_p , for each prime p , of congruence classes of $\mathbb{Z} \bmod p$.
- The *algebraic number fields* of Dedekind and Kronecker, which are subfields of \mathbb{C} consisting of algebraic numbers.

In particular, Dedekind (1871) viewed fields of algebraic numbers as *vector spaces over \mathbb{Q}* , and singled out those of finite dimension. Kronecker went so far as to claim that an algebraic number is properly realized *by* a field, and that existence of these fields is the proper *fundamental theorem of algebra*, as we will see in Section 16.6.

The existence of the finite fields \mathbb{F}_p is an easy consequence of the Euclidean algorithm in \mathbb{Z} , which was touched on in Section 14.1. We review the argument here because it is the prototype for the construction of algebraic number fields, which we come back to in Section 16.6. The path from \mathbb{Z} , and a prime p , to the field \mathbb{F}_p goes as follows.

1. The members of \mathbb{F}_p are the classes $[0], [1], [2], \dots, [p-1]$ defined by congruence mod p :

$$[a] = \{n : n \equiv a \pmod{p}\} = \{\dots, a-p, a, a+p, a+2p, \dots\}.$$

2. Congruence classes are added and multiplied by the rules

$$[a] + [b] = [a + b], \quad [a][b] = [ab].$$

It must be checked that sum and product of congruence classes are well-defined; that is, they do not depend on the numbers a, b chosen to represent their congruence classes. But once this is done all the field properties, except the existence of inverses, follow easily from the corresponding properties of sum and product for integers.

3. If $[a] \neq [0]$ we find an inverse of the class $[a]$ by the Euclidean algorithm. Since p is prime, $\gcd(a, p) = 1$, and the Euclidean algorithm then gives integers m and n such that

$$1 = \gcd(a, p) = ma + np.$$

4. In other words, $ma \equiv 1 \pmod{p}$, so

$$[m][a] = [1],$$

and hence $[a]$ has the inverse $[m]$.

Vector Spaces over a Field

If \mathbb{F} is any field the definition of a *vector space over \mathbb{F}* is identical with the definition in Section 16.2, except that the scalars a, b, c, \dots now come from \mathbb{F} . In the next two sections we will be particularly interested in vector spaces over the field \mathbb{Q} of rational numbers.

\mathbb{Q} , as remarked above, is the field of basic arithmetic, so the most concrete way to approach the *irrational* numbers arising from polynomial equations is to view them in relation to rational numbers where possible. As we will see in the next section, this can be done for the numbers α that satisfy polynomial equations with rational coefficients—the so-called *algebraic numbers*. In this case, α belongs to a vector space of finite dimension over \mathbb{Q} .

EXERCISES

16.3.1 Find the inverses of $[1], [2], [3], [4] \pmod{5}$.

16.3.2 Explain why congruence classes mod 6 do *not* form a field under addition and multiplication of congruence classes.

16.4 Algebraic Numbers and Algebraic Integers

An *algebraic number* may be defined as one that satisfies a polynomial equation $p(x) = 0$ with coefficients in \mathbb{Q} . Without loss of generality we can assume this equation is of the form

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0, \quad \text{where } a_0, a_1, \dots, a_{n-1} \in \mathbb{Q}. \quad (*)$$

An algebraic number is said to be of *degree* n if it satisfies such a polynomial equation of degree n but not one of lower degree. Thus $\sqrt{2}$, for example, is of degree 2 because it satisfies the equation $x^2 - 2 = 0$ but not any equation of the form $ax + b = 0$ with $a, b \in \mathbb{Q}$, since the latter equation would imply that $\sqrt{2}$ is rational.

An algebraic number α satisfies only one polynomial equation of minimal degree and of the form (*). If there were two such equations their difference would be of lower degree, yet also satisfied by α . We call $p(x)$ the *minimal polynomial* for α . The minimal polynomial $p(x)$ is necessarily *prime*, or *irreducible*, because any factors of $p(x)$ would give a lower-degree polynomial also satisfied by α .

This leads, as we will see in Section 16.6, to a close analogy between integers modulo a prime p and polynomials modulo an irreducible $p(x)$. In particular, the analogy gives the existence of polynomial inverses mod $p(x)$, which clarifies the nature of inverses among the algebraic numbers.

Generating a Field from an Algebraic Number

Each algebraic number α gives rise to a field $\mathbb{Q}(\alpha)$, which can be viewed as the smallest field containing \mathbb{Q} and the number α .

$\mathbb{Q}(\alpha)$ consists of all quotients $q(\alpha)/r(\alpha)$, where q and r are polynomials with coefficients in \mathbb{Q} . It follows that the sum, difference, product, and quotient (with nonzero denominator) of any members of $\mathbb{Q}(\alpha)$ is itself a member of $\mathbb{Q}(\alpha)$. It is also clear that all members belong to \mathbb{C} , which has the field properties, so $\mathbb{Q}(\alpha)$ has them too. Thus $\mathbb{Q}(\alpha)$ is a *field*, clearly containing α and all members of \mathbb{Q} . Conversely, any number obtainable from α and members of \mathbb{Q} by sums, differences, products, and quotients is a member of $\mathbb{Q}(\alpha)$. That is, any field containing α and \mathbb{Q} contains $\mathbb{Q}(\alpha)$. In this sense, $\mathbb{Q}(\alpha)$ is the “smallest” such field.

In Section 16.6 we will see that $\mathbb{Q}(\alpha)$ may also be fruitfully viewed as a vector space. In particular, $\mathbb{Q}(\sqrt{2})$ is a vector space over \mathbb{Q} with basis elements 1 and $\sqrt{2}$, as can be checked in the exercises below.

It is not obvious, at this stage, whether all members of $\mathbb{Q}(\alpha)$ are algebraic numbers. Indeed it is not obvious whether $\alpha + \beta$ is an algebraic number when α and β are. The same question can be asked of the algebraic *integers* to which we now turn.

Algebraic Integers

In analogy with the definition of algebraic number, we define an *algebraic integer* to be a solution of an equation of the form (called *monic* because the leading coefficient is 1)

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0, \quad \text{where } a_0, a_1, \dots, a_{n-1} \in \mathbb{Z}. \quad (**)$$

This definition includes some numbers that look like integers, such as the *Gaussian integers* $a + b\sqrt{-1}$, where $a, b \in \mathbb{Z}$, but also some that do not, such as $\frac{-1+\sqrt{-3}}{2}$, which is a solution of $x^3 - 1 = 0$. Nevertheless, it turns out that algebraic integers are the right counterpart of ordinary integers among the algebraic numbers. In particular, the algebraic integers among the rational numbers are the ordinary integers. The definition (**) was proposed by Dedekind (1871), in the light of extensive experience with algebraic numbers. Another piece of evidence that supports (**) is the result of Eisenstein (1850) that sums and products of numbers satisfying (**) are also numbers of this form.

An interesting feature of Eisenstein's result is the use of determinant theory, from the hard core of Leibniz-era linear algebra that modern linear algebra tries to avoid. For those familiar with determinants, the argument is outlined in the exercises below. The corresponding result about sum and product of algebraic numbers, as we will see in the next three sections, is obtainable by softer methods.

EXERCISES

- 16.4.1** Show that the sum, difference, and product of numbers of the form $a + b\sqrt{2}$ are again of this form, and so is $\frac{1}{a+b\sqrt{2}}$.
- 16.4.2** Deduce from Exercise 16.4.1 that $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.
- 16.4.3** Prove that $x = \sqrt{2} + \sqrt{3}$ is an algebraic integer by finding a suitable fourth-degree polynomial satisfied by x .

16.4.4 Suppose that $x = r/s$ is a rational algebraic integer, so that

$$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1\frac{r}{s} + a_0 = 0 \quad \text{where } a_0, a_1, \dots, a_{n-1} \in \mathbb{Z}.$$

Deduce that r^n is divisible by s .

16.4.5 Assuming now that $\gcd(r, s) = 1$ in Exercise 16.4.4, conclude that $s = 1$, and hence that x is an ordinary integer.

We now prove that the sum of algebraic integers is an algebraic integer. Suppose α satisfies an equation $\alpha^k + a_{k-1}\alpha^{k-1} + \cdots + a_1\alpha + a_0 = 0$, with $a_0, a_1, \dots, a_{k-1} \in \mathbb{Z}$.

16.4.6 Observing that

$$\begin{aligned} \alpha^k &= -a_{k-1}\alpha^{k-1} - \cdots - a_1\alpha - a_0, \\ \alpha^{k+1} &= -a_{k-1}\alpha^k - \cdots - a_1\alpha^2 - a_0\alpha, \\ &\vdots \end{aligned}$$

and so on, explain why every polynomial in α with integer coefficients is a linear combination of $1, \alpha, \alpha^2, \dots, \alpha^{k-1}$ with coefficients in \mathbb{Z} .

Similarly, if β satisfies a monic polynomial equation of degree l , any polynomial in β is a linear combination of $1, \beta, \dots, \beta^{l-1}$ with integer coefficients. Consequently, *any polynomial in α and β is a linear combination of terms $\alpha^i\beta^j$, with $0 \leq i \leq k-1$ and $0 \leq j \leq l-1$, with integer coefficients.*

Denoting the kl products $\alpha^i\beta^j$ by $\omega_1, \dots, \omega_{kl}$ conclude that we can write each polynomial ω in α and β (such as $\alpha \pm \beta$ or $\alpha\beta$) in the form

$$\omega = n_1\omega_1 + \cdots + n_{kl}\omega_{kl} \quad \text{where } n_1, \dots, n_{kl} \in \mathbb{Z}. \quad (*)$$

16.4.8 Deduce from (*) that ω satisfies kl equations in the kl unknowns ω_m with integer coefficients:

$$\begin{aligned} \omega\omega_1 &= n'_1\omega_1 + \cdots + n'_{kl}\omega_{kl} \\ \omega\omega_2 &= n''_1\omega_1 + \cdots + n''_{kl}\omega_{kl} \\ &\vdots \\ \omega\omega_{kl} &= n^{(kl)}_1\omega_1 + \cdots + n^{(kl)}_{kl}\omega_{kl}. \end{aligned}$$

16.4.9 Conclude that these equations have nonzero determinant, that is,

$$\det \begin{pmatrix} n'_1 - \omega & n'_2 & \cdots & n'_{kl} \\ n''_1 & n''_2 - \omega & \cdots & n''_{kl} \\ \vdots & \vdots & \ddots & \vdots \\ n^{(kl)}_1 & n^{(kl)}_2 & \cdots & n^{(kl)}_{kl} - \omega \end{pmatrix} = 0.$$

Explain why this shows that ω is an algebraic integer.

16.5 Rings

The ring axioms are modelled on the properties of the ordinary integers:

$$\begin{array}{lll}
 a + b = b + a & ab = ba & \text{(commutative laws)} \\
 a + (b + c) = (a + b) + c & a(bc) = (ab)c & \text{(associative laws)} \\
 a + (-a) = 0 & & \text{(inverse law)} \\
 a + 0 = a & a \cdot 1 = a & \text{(identity laws)} \\
 a(b + c) = ab + ac & & \text{(distributive law)}
 \end{array}$$

These *ring axioms* were formulated to capture the common properties of ordinary integers and the algebraic integers defined in Section 16.4. Special cases of algebraic integers were first introduced by Euler and Gauss to solve problems about ordinary integers.

For example, Euler (1770b) used “integers” of the form $a + b\sqrt{-2}$, for ordinary integers a and b , to find the ordinary integer solutions of

$$y^3 = x^2 + 2.$$

His idea was to factorize the right hand side as $(x + \sqrt{-2})(x - \sqrt{-2})$ and to argue that $x + \sqrt{-2}$ and $x - \sqrt{-2}$ behave like relatively prime integers. Then, assuming that unique prime factorization holds among the “integers” $a + b\sqrt{-2}$, it follows that both $x + \sqrt{-2}$ and $x - \sqrt{-2}$ are cubes, and a simple calculation leads to the single positive solution $x = 5$, $y = 3$. (See the exercises below.)

This spectacular extension of classical arithmetic reasoning to new kinds of “integer” prompts a broader definition of integers, and a study of the primes among them. The ring axioms capture the fundamental properties of integers, but they do *not* imply unique prime factorization. Section 16.8 discusses how to refine the ring concept so as to ensure unique prime factorization, but first we will deal with an important case where unique prime factorization holds: a *polynomial ring over a field*, $\mathbb{F}[x]$.

Polynomial Rings

Polynomials have been studied since the invention of algebraic notation. As early as 1585 Stevin observed that they behave like integers in an important way: they enjoy “division with remainder” in the following sense. If $a(x)$ and $b(x) \neq 0$ are polynomials then there is a “quotient” polynomial

$q(x)$ and “remainder” polynomial $r(x)$ such that

$$a(x) = b(x)q(x) + r(x),$$

and $r(x)$ is “smaller” than $b(x)$ in the sense of having lower degree (with the special case that 0 is taken to have lower degree than a nonzero constant).

To see why division property holds, suppose that

$$\begin{aligned} a(x) &= a_n x^n + \cdots + a_1 x + a_0, \\ b(x) &= b_m x^m + \cdots + b_1 x + b_0 \end{aligned}$$

with $m \leq n$ (otherwise $a(x)$ itself can serve as $r(x)$, with $q(x) = 0$). In this case $a(x) - b(x) \cdot \frac{a_n}{b_m} x^{n-m}$ is a polynomial $a'(x)$ of degree $n' < n$, because the subtraction removes the term $a_n x^n$ in $a(x)$. Then if $m \leq n'$ we can repeat the process, eventually obtaining a polynomial $r(x)$ of degree $< m$. The various multipliers of $b(x)$ used in this process add up to the quotient $q(x)$.

Notice that we use only addition, subtraction, multiplication, and division of coefficients, so the division property holds for polynomials with coefficients from any field \mathbb{F} . These polynomials form a ring called $\mathbb{F}[x]$.

Now that we have the division property for $\mathbb{F}[x]$, a Euclidean algorithm follows, along with all its usual consequences:

- Any polynomials $a(x)$ and $b(x)$ have a divisor $\gcd(a(x), b(x))$ which is greatest in the sense that it is divisible by any other polynomial dividing both $a(x)$ and $b(x)$.
- $\gcd(a(x), b(x)) = m(x)a(x) + n(x)b(x)$ for some polynomials $m(x), n(x)$ in $\mathbb{F}[x]$.
- If $p(x)$ is an irreducible polynomial, and $a(x)$ does not divide $p(x)$, then $\gcd(a(x), p(x)) = 1$ (or any other nonzero member of \mathbb{F} , since all of them divide 1).
- (*Prime divisor property*) If $p(x)$ is an irreducible polynomial that divides $a(x)b(x)$, then $p(x)$ divides $a(x)$ or $p(x)$ divides $b(x)$.
- (*Unique prime factorization*) Any polynomial in $\mathbb{F}[x]$ has a factorization into irreducibles, which is unique up to the order of factors and nonzero factors from \mathbb{F} .

In particular, polynomials in $\mathbb{Q}[x]$ have factorization into irreducibles, which is unique up to the order of factors and nonzero rational factors.

EXERCISES

Determining whether a polynomial in $\mathbb{Q}[x]$ is irreducible is often a difficult problem, but in low-degree cases we can appeal to proofs that certain numbers are irrational.

16.5.1 Prove that $\sqrt[3]{2}$ is irrational and deduce that $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$.

Here is part of Euler's solution of $y^3 = x^2 + 2$, using the integers $a + b\sqrt{-2}$ and assuming their unique prime factorization.

16.5.2 Assuming $x + \sqrt{-2} = (a + b\sqrt{-2})^3$ for $a, b \in \mathbb{Z}$, equate real and imaginary parts to find the only positive integer solution of $y^3 = x^2 + 2$.

Unique prime factorization in $\mathbb{Z}[\sqrt{-2}]$ is proved, as in \mathbb{Z} , by proving a *division property*—which yields a Euclidean algorithm, prime divisor property, and hence unique prime factorization. We illustrate the idea first with the Gaussian integers $\mathbb{Z}[i]$, the smaller members of which are shown as dots in Figure 16.2. The figure also shows the *multiples of $3 + i$* among them as black dots, and the particular Gaussian integer $5 + 3i$ as a gray dot.

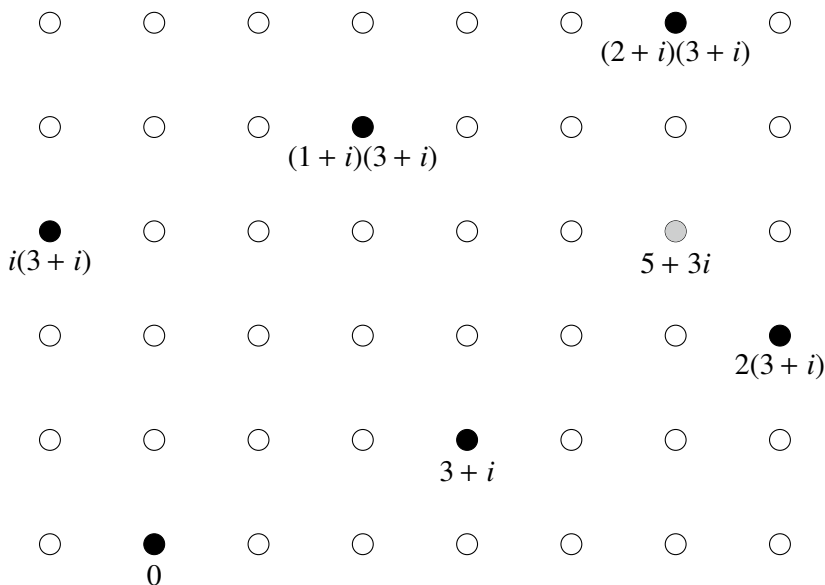


Figure 16.2: Multiples of $3 + i$ near $5 + 3i$

- 16.5.3** Explain why the multiples of $3 + i$ form an array of squares, like the array $\mathbb{Z}[i]$ itself but magnified and rotated.
- 16.5.4** Explain in general why the multiples $\mu\beta$ of a Gaussian integer β form an array of squares, each of side length $|\beta|$.
- 16.5.5** Show also that any Gaussian integer α (such as $5 + 3i$) lies at distance $|\alpha - \mu\beta| < |\beta|$ from the nearest multiple of β .
- 16.5.6** Deduce from Exercise 16.5.5 that, for any Gaussian integers α and $\beta \neq 0$, there are Gaussian integers μ, ρ with the *division property*:

$$\alpha = \mu\beta + \rho, \quad \text{where } |\rho| < |\beta|.$$

- 16.5.7** Show similarly that $\mathbb{Z}[\sqrt{-2}]$ has the division property, and hence unique prime factorization.

16.6 Fields as Vector Spaces

Now suppose that α is an algebraic number with minimal polynomial $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ of degree n . We notice that

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha + a_0$$

and, more generally, any higher power of α is a linear combination of $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ with rational coefficients.

So the set $\mathbb{Q}[\alpha]$ of all polynomials in α with rational coefficients, which is clearly a vector space, in fact equals the set of rational combinations of $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$, which is a vector space of *dimension* n over \mathbb{Q} . We have just seen that the elements $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ span $\mathbb{Q}[\alpha]$, and they are linearly independent because an equation

$$b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0, \quad \text{with } b_0, b_1, \dots, b_{n-1} \in \mathbb{Q} \text{ not all zero,}$$

contradicts the assumption that α has degree n .

Moreover, *the vector space $\mathbb{Q}[\alpha]$ is a field*. It is clear that the sum, difference, and product of any two members of $\mathbb{Q}[\alpha]$ also belongs to $\mathbb{Q}[\alpha]$. Thus it remains to show that the inverse β^{-1} of any $\beta \in \mathbb{Q}[\alpha]$ is also a member. We do this in the same way we found inverses mod p in the previous section, by considering the relation of *congruence mod $p(x)$* and appealing to the Euclidean algorithm for polynomials.

Congruence Modulo an Irreducible Polynomial

Instead of the ring \mathbb{Z} and a prime $p \in \mathbb{Z}$, we now take the ring $\mathbb{Q}[x]$ of polynomials with rational coefficients and an irreducible polynomial $p(x) \in \mathbb{Q}[x]$. We introduce the notion of *congruence mod $p(x)$* by saying

$$a(x) \equiv b(x) \pmod{p(x)}$$

if $p(x)$ divides $a(x) - b(x)$. This gives *congruence classes of polynomials*, $[a(x)]$, which can be added and multiplied by the rules

$$[a(x)] + [b(x)] = [a(x) + b(x)] \quad \text{and} \quad [a(x)] \cdot [b(x)] = [a(x) \cdot b(x)].$$

We verify, exactly as we did for congruence classes of numbers modulo a prime in Section 16.3, that this sum and product are well defined and have the ring properties.

Finally, and again by the same argument as in Section 16.3, using the Euclidean algorithm, we find that each nonzero class $[a(x)]$ has an *inverse* class $[m(x)]$, in the sense that

$$[m(x)][a(x)] = [1].$$

Thus *the ring of congruence classes of polynomials in $\mathbb{Q}[x]$, modulo an irreducible $p(x)$, is a field*. We now return to the vector space $\mathbb{Q}[\alpha]$ to claim that its members are *essentially the same* as congruence classes of polynomials in $\mathbb{Q}[x] \bmod p(x)$, so $\mathbb{Q}[\alpha]$ is also a field.

In fact, we get a one-to-one correspondence between the congruence classes and elements of $\mathbb{Q}[\alpha]$ by letting each $[r(x)]$ correspond to $r(\alpha)$. This correspondence is one-to-one because, for any polynomial $t(x) \in \mathbb{Q}[x]$,

$$p(x) \text{ divides } t(x) \Leftrightarrow t(\alpha) = 0.$$

The direction \Rightarrow is clear because $p(\alpha) = 0$. Conversely, suppose $t(\alpha) = 0$ and consider the result of dividing $t(x)$ by $p(x)$. By the division property,

$$t(x) = q(x)p(x) + r(x),$$

where $r(x)$ has lower degree than $p(x)$. Then, since $t(\alpha)$ and $p(\alpha)$ are 0, $r(\alpha) = 0$ also. This contradicts the minimality of $p(x)$, unless $r(x) = 0$, in which case $p(x)$ divides $t(x)$. It follows now that, for any $u(x), v(x) \in \mathbb{Q}[x]$,

$$\begin{aligned} u(x) \text{ and } v(x) \text{ are in the same class} &\Leftrightarrow p(x) \text{ divides } u(x) - v(x) \\ &\Leftrightarrow u(\alpha) - v(\alpha) = 0 \\ &\Leftrightarrow u(\alpha) = v(\alpha). \end{aligned}$$

so congruence classes mod $p(x)$ correspond to values in $\mathbb{Q}[\alpha]$.

Revisiting the Fundamental Theorem of Algebra

The proof above realizes the field $\mathbb{Q}[\alpha]$, where α is typically irrational or imaginary, by a concrete collection of *rational* objects; namely, polynomials with rational coefficients. For example, the field $\mathbb{Q}(\sqrt{2})$ involving the irrational number $\sqrt{2}$ is, for all algebraic purposes, the same as the collection of linear polynomials $ax + b$, where $a, b \in \mathbb{Q}$. These polynomials are added and multiplied in the usual way with the proviso that $x^2 - 2 = 0$, and $\sqrt{2}$ itself corresponds to the congruence class of x .¹

The general idea of replacing algebraic numbers, and the fields they generate, by congruence classes of rational polynomials, was proposed by Kronecker (1887). Kronecker was opposed to irrational numbers, to large infinite totalities like \mathbb{R} and \mathbb{C} , and especially to pure existence proofs, where objects were shown to exist without being constructed. For all these reasons he objected to the fundamental theorem of algebra. He believed that it should be replaced by what he called the “fundamental theorem of general arithmetic,” an instance of which is the realization of $\mathbb{Q}(\alpha)$ by the field of congruence classes mod $p(x)$ in $\mathbb{Q}[x]$.

This field, though infinite, can be constructed step by step using only rational numbers, and it contains a solution to the polynomial equation $p(x) = 0$, namely the equivalence class of x , mod $p(x)$. Thus, if one prefers a fundamental theorem in which roots of polynomial equations are constructed as simply as possible, congruence classes of rational polynomials are the way to go. For more on Kronecker’s view of the fundamental theorem of algebra, see Edwards (2007).

EXERCISES

16.6.1 Prove that $\mathbb{Q}(2^{1/3}) = \{a + b2^{1/3} + c2^{2/3} : a, b, c \in \mathbb{Q}\}$.

16.7 Fields of Algebraic Numbers

As we mentioned in Section 16.4, it is not obvious that $\alpha + \beta$ is an algebraic number when α and β are. One proof of this fact uses determinants, but a simpler proof follows from a general theorem about the dimension of vector spaces pointed out by Dedekind (1894).

¹In a similar way the field of complex numbers is realized by *real* linear polynomials $a + bx$ with the proviso that $x^2 + 1 = 0$. The latter example was actually proposed by Cauchy (1847) as a rigorous approach to complex numbers.

Dimension Theorem. For fields $\mathbb{D} \subseteq \mathbb{E} \subseteq \mathbb{F}$, with \mathbb{E} of dimension m over \mathbb{D} and \mathbb{F} of dimension n over \mathbb{E} , \mathbb{F} has dimension mn over \mathbb{D} .

Proof. If e_1, e_2, \dots, e_m is a basis for \mathbb{E} over \mathbb{D} , each $e \in \mathbb{E}$ can be written

$$e = d'_1 e_1 + d'_2 e_2 + \cdots + d'_m e_m \quad \text{for some } d'_1, d'_2, \dots, d'_m \in \mathbb{D}.$$

Likewise, if f_1, f_2, \dots, f_n is a basis for \mathbb{F} over \mathbb{E} , each $f \in \mathbb{F}$ can be written

$$f = e'_1 f_1 + e'_2 f_2 + \cdots + e'_n f_n \quad \text{for some } e'_1, e'_2, \dots, e'_n \in \mathbb{E}.$$

These equations imply any $f \in \mathbb{F}$ can be written as a linear combination of the elements $e_i f_j$ with coefficients $d_{ij} \in \mathbb{D}$.

Thus the mn elements $e_i f_j$ span \mathbb{F} over \mathbb{D} . Also, they are linearly independent. Supposing

$$\begin{aligned} 0 &= d_{11} e_1 f_1 + d_{12} e_1 f_2 + \cdots + d_{1n} e_1 f_n \\ &\quad + d_{21} e_2 f_1 + d_{22} e_2 f_2 + \cdots + d_{2n} e_2 f_n \\ &\quad \vdots \\ &\quad + d_{m1} e_m f_1 + d_{m2} e_m f_2 + \cdots + d_{mn} e_m f_n \end{aligned}$$

it follows, since f_1, f_2, \dots, f_n are linearly independent over \mathbb{E} , that their coefficients are zero. That is

$$\begin{aligned} 0 &= d_{11} e_1 + d_{21} e_2 + \cdots + d_{m1} e_m \\ 0 &= d_{12} e_1 + d_{22} e_2 + \cdots + d_{m2} e_m \\ &\quad \vdots \\ 0 &= d_{1n} e_1 + d_{2n} e_2 + \cdots + d_{mn} e_m \end{aligned}$$

which in turn implies each $d_{ij} = 0$, because e_1, e_2, \dots, e_m are linearly independent over \mathbb{D} . \square

To apply this theorem we suppose α is an algebraic number of degree m , so $\mathbb{Q}[\alpha]$ is a vector space of dimension m over \mathbb{Q} . Now if β is an algebraic number of degree n then the vector space

$$(\mathbb{Q}[\alpha])[\beta] = \{\text{polynomials in } \beta \text{ with coefficients in } \mathbb{Q}[\alpha]\}$$

has dimension *at most* n over the field $\mathbb{Q}[\alpha]$ because β^n is a linear combination of $1, \beta, \beta^2, \dots, \beta^{n-1}$ with *rational* coefficients, hence certainly with coefficients in $\mathbb{Q}[\alpha]$. The same applies to the higher powers $\beta^{n+1}, \beta^{n+2}, \dots$, by the argument used in Section 16.6. Thus the elements $1, \beta, \beta^2, \dots, \beta^{n-1}$ span $(\mathbb{Q}[\alpha])[\beta]$, which therefore has dimension $\leq n$ as a vector space over $\mathbb{Q}[\alpha]$.

It follows, by the dimension theorem, that the dimension of $(\mathbb{Q}[\alpha])[\beta]$ over \mathbb{Q} is at most mn . Now $\alpha + \beta$ clearly belongs to $(\mathbb{Q}[\alpha])[\beta]$, so it is algebraic, of degree $\leq mn$, by the following simple theorem.

Field of finite dimension over \mathbb{Q} . *In a field of \mathbb{F} dimension d over \mathbb{Q} , each element is an algebraic number of degree $\leq d$.*

Proof. If $\gamma \in \mathbb{F}$, where \mathbb{F} has dimension d over \mathbb{Q} , the $d + 1$ elements $1, \gamma, \gamma^2, \dots, \gamma^d$ cannot be linearly independent. Hence there are rational numbers a_0, a_1, \dots, a_d , *not all zero*, such that

$$a_0 + a_1\gamma + \dots + a_d\gamma^d = 0.$$

This equation shows that γ is algebraic, of degree $\leq d$. □

This argument has consequences both for the “small” fields $\mathbb{Q}(\alpha)$ of Section 16.4, each generated by a single algebraic number, and the collection of all algebraic numbers.

Corollary 1 *When α is an algebraic number, all members of $\mathbb{Q}(\alpha)$ are algebraic.*

Proof. If α is of degree d , then $\mathbb{Q}(\alpha)$ equals the vector space $\mathbb{Q}[\alpha]$ of dimension d over \mathbb{Q} by the argument in Section 16.6. Then each member of $\mathbb{Q}(\alpha)$ is an algebraic number of degree $\leq d$ by the theorem above. □

Corollary 2 *The set of all algebraic numbers is closed under the operations $+$, $-$, \times , and \div (by nonzero elements), and hence is a field.*

Proof. If α and $\beta \neq 0$ are algebraic numbers then not only $\alpha + \beta$ but also $\alpha - \beta, \alpha\beta$, and α/β belong to $(\mathbb{Q}[\alpha])[\beta]$, which is of finite dimension over \mathbb{Q} . Hence they are algebraic by the theorem above. □

EXERCISES

An algebraic problem originating in Euclid’s geometry is the problem of *constructible numbers*. Geometrically speaking, a number is α constructible if the corresponding length is constructible from the unit length by ruler and compass.

With the arithmetization of geometry by Descartes (1637), we saw in the exercises to Section 5.3 that an equivalent algebraic statement is that α is obtainable from 1 by the rational operations $+, -, \times, \div$ and the $\sqrt{}$ operation. We can now revisit the question of whether $\sqrt[3]{2}$ is constructible, first solved in the exercises to Section 5.4.

16.7.1 Explain why an equivalent question is whether there are fields

$$\mathbb{Q} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_k,$$

with each \mathbb{F}_{n+1} of dimension 2 over \mathbb{F}_n and $\sqrt[3]{2} \in \mathbb{F}_k$.

16.7.2 Deduce from the dimension theorem that $\mathbb{Q}(\alpha)$ has dimension 2^k , for some $k \geq 0$, when α is a constructible number, and that α has degree 2^k .

16.7.3 Conclude, with the help of Exercise 16.5.1, that $\sqrt[3]{2}$ is not constructible.

16.8 Ideals

As we saw in the exercises to Section 16.4, if α and β are algebraic integers, then so are $\alpha + \beta$, $\alpha - \beta$, and $\alpha\beta$. Thus the set of all algebraic integers is closed under the operations of $+$, $-$, and \times , and hence it is a ring. But it is not a good ring for doing arithmetic, because it has no “primes”: if α is an algebraic integer then so is $\sqrt{\alpha}$, hence every algebraic integer has a nontrivial factorization $\alpha = \sqrt{\alpha} \sqrt{\alpha}$.

Dedekind (1871) found that the right setting for arguments about algebraic integers and primes, such as Euler’s solution of the equation $y^3 = x^2 + 2$ mentioned in Section 16.5, is in fields of finite dimension over \mathbb{Q} . Euler’s solution uses the algebraic integers in the two-dimensional field $\mathbb{Q}[\sqrt{-2}]$, which happen to be precisely the numbers of the form $a + b\sqrt{-2}$, where $a, b \in \mathbb{Z}$.

In this example, one can prove that unique prime factorization holds in $\mathbb{Q}[\sqrt{-2}]$ with the help of a measure of size for the integers $a + b\sqrt{-2}$ called their *norm*:

$$\text{norm}(a + b\sqrt{-2}) = a^2 + 2b^2$$

This norm is simply the square of the absolute value $|a + b\sqrt{-2}|$, and hence it has the *multiplicative* property:

$$\text{norm}(\alpha\beta) = \text{norm}(\alpha)\text{norm}(\beta).$$

We call an algebraic integer of $\mathbb{Q}[\sqrt{-2}]$ *prime* if it has norm greater than 1 and is not the product of algebraic integers of smaller norm. The *existence* of prime factorization then follows as in \mathbb{Z} . Since norms are ordinary

positive integers, the process of splitting an integer into factors of smaller norm must terminate—since positive integers cannot decrease forever—necessarily in factors that are prime.

The situation is the same in any algebraic number field of finite dimension. Dedekind (1871) showed that each such field has a concept of norm, which is multiplicative and integer-valued for algebraic integers, so primes and prime factorizations exist. However, prime factorization is *not* always unique. Euler (1770b) was lucky to pick $\mathbb{Q}[\sqrt{-2}]$, because it does indeed have unique prime factorization, as we showed in Exercise 16.5.7. On the other hand, $\mathbb{Q}[\sqrt{-5}]$ does not.

In $\mathbb{Q}[\sqrt{-5}]$ the integers are the numbers of the form $a + b\sqrt{-5}$, where $a, b \in \mathbb{Z}$, among which the integer 6 has the factorizations

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

The norm of $a + b\sqrt{-5}$ is $a^2 + 5b^2$, and it can be checked that each of 2, 3, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$ is prime according to this norm, so the number 6 has two distinct prime factorizations.

Failure of unique prime factorization among the algebraic integers was first noticed by Kummer in the 1840s, and he realized that it is a serious problem. He wrote:

It is greatly to be lamented that this virtue of the real numbers [that is, of the ordinary integers] to be decomposable into prime factors, always the same ones for a given number, does not also belong to the complex numbers [that is, the algebraic integers]; were this the case, the whole theory, which is still laboring under such difficulties, could easily be brought to a conclusion. For this reason, the complex numbers we have been considering seem imperfect, and one may well ask whether one ought not to look for another kind which would preserve the analogy with the real numbers with respect to such a fundamental property.

Translation by Weil (1975) from Kummer (1844)

Dedekind (1877) put himself in Kummer's shoes as he described this turning point in the history of algebra:

But the more hopeless one feels about the prospects of later research on such numerical domains, the more one has to

admire the steadfast efforts of Kummer, which were finally rewarded by a truly great and fruitful discovery.

Dedekind (1877), p. 56.

Kummer found “another kind” of number that overcame the failure of unique prime factorization, and he called them *ideal numbers*, though he did not properly define them. Today we know them under the concept of *ideals*, introduced by Dedekind (1871) to formalize Kummer’s idea, and to generalize it to all rings of algebraic integers in algebraic number fields of finite dimension. The idea, roughly speaking, is that a number may be known by its set of multiples. Dedekind realized that a set I of multiples in a ring R has two key properties:

- If $\alpha, \beta \in I$ then $\alpha + \beta \in I$.
- If $\alpha \in I$ and $\rho \in R$ then $\rho\alpha \in I$.

He made these the defining properties of an *ideal* I in a ring R .

Ideals first showed their fruitfulness in number theory, where they allowed algebraic integers to be used freely while preserving the analogy with ordinary integers. But ideals soon found other applications, starting with their use by Dedekind and Weber (1882) in algebraic geometry, where they are applied to fields of algebraic functions. Today, ideals are such a fundamental part of ring theory that algebra books often introduce them without explaining that the word “ideal” came from “ideal numbers.”

EXERCISES

16.8.1 Show that $\{4m : m \in \mathbb{Z}\}$ and $\{6n : n \in \mathbb{Z}\}$ are ideals in \mathbb{Z} .

16.8.2 Show also that $\{4m + 6n : m, n \in \mathbb{Z}\}$ is an ideal, which equals $\{2k : k \in \mathbb{Z}\}$.

16.9 Ideal Prime Factorization

To see how ideals of algebraic integers might preserve the analogy with ordinary integers, we begin by rewriting the theory of divisibility and gcd in \mathbb{Z} in terms of ideals. This suggests appropriate definitions of divisor and gcd for ideals of algebraic integers, and leads to the discovery that the two factorizations

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

arise from a single *ideal prime factorization*, as Kummer hoped.

Ideals in \mathbb{Z}

In \mathbb{Z} we have the commonplace facts that

$$2 \text{ divides } 6, \quad 3 \text{ divides } 6, \quad \gcd(2, 3) = 1.$$

These facts can be rewritten in terms of the sets

$$(2) = \{\text{multiples of } 2\}, \quad (3) = \{\text{multiples of } 3\}, \quad (6) = \{\text{multiples of } 6\},$$

which are examples of ideals. The equivalents of the first two facts are

$$(2) \text{ contains } (6), \quad (3) \text{ contains } (6),$$

which may be summed up by the slogan *to divide is to contain*. To express the third fact we consider another ideal, the *sum* of (2) and (3) :

$$(2) + (3) = \{a + b : a \in (2), b \in (3)\}.$$

It is clear that $\gcd(2, 3)$ divides any member of the set $(2) + (3)$, and in fact it is not hard to show that

$$(2) + (3) = \{\text{multiples of } 1\} = (1) = (\gcd(2, 3)).$$

In general, for any $a \in \mathbb{Z}$, the set $(a) = \{\text{multiples of } a\}$ is obviously an ideal, called the *principal ideal* generated by a . It is not hard to prove (see the exercises below) that

- every ideal in \mathbb{Z} is (a) for some a ,
- $a \text{ divides } b \Leftrightarrow (a) \text{ contains } (b)$,
- $(a) + (b) = (\gcd(a, b))$.

Since ideals in \mathbb{Z} correspond to numbers in \mathbb{Z} , the language of ideals tells us nothing new about \mathbb{Z} . However, the concept of ideal gives us new insight into the ring $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$, where *not* every ideal is principal.

Ideals in $\mathbb{Z}[\sqrt{-5}]$

One such ideal is the sum I of the principal ideals (2) and $(1 + \sqrt{-5})$, $\{2\mu + (1 + \sqrt{-5})\nu : \mu, \nu \in \mathbb{Z}[\sqrt{-5}]\}$, which happens to equal

$$\{2m + (1 + \sqrt{-5})n : m, n \in \mathbb{Z}\}.$$

We expect (by analogy with \mathbb{Z}) this ideal to be the gcd of the principal ideals (2) and $(1 + \sqrt{-5})$. In Kummer's terms it is the set of multiples of the "ideal number" $\gcd(2, 1 + \sqrt{-5})$. It can be seen from a picture of part of I (the black dots in Figure 16.3) that I is *not* a principal ideal.

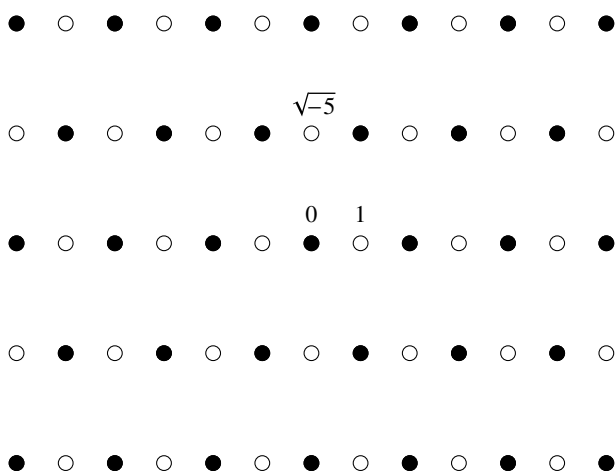


Figure 16.3: Multiples of $\gcd(2, 1 + \sqrt{-5})$

This is because a principal ideal (α) in $\mathbb{Z}[\sqrt{-5}]$ is simply $\mathbb{Z}[\sqrt{-5}]$ multiplied by α , so it looks like the rectangular array $\mathbb{Z}[\sqrt{-5}]$, only magnified by $|\alpha|$ and rotated by the argument of α . In particular, *a principal ideal is a rectangular array*. But it is clear from Figure 16.3 that the black dots do not form rectangles.

It can be seen similarly that the ideals $(3) + (1 + \sqrt{-5}) = (\gcd(3, 1 + \sqrt{-5}))$ and $(3) + (1 - \sqrt{-5}) = (\gcd(3, 1 - \sqrt{-5}))$ are not principal ideals. But these ideals are plausible *ideal factors* of the numbers $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ found in the two factorizations of 6. We have only to explain what it means to *multiply* ideals.

Product of Ideals

Dedekind (1871) defined the product of ideals A, B to consist of all finite sums of products $a_i b_i$, where $a_i \in A$ and $b_i \in B$. Thus

$$AB = \{a_1 b_1 + \cdots + a_n b_n : a_1, \dots, a_n \in A; b_1, \dots, b_n \in B\}.$$

This concept of product agrees with the idea that “to divide is to contain” because each $a_i b_i \in A$ and hence $a_1 b_1 + \cdots + a_n b_n \in A$, so $A \supseteq AB$ and therefore A divides AB . Similarly, B divides AB .

The ideals

$$A = (2) + (1 + \sqrt{-5}), \quad B = (3) + (1 + \sqrt{-5}), \quad \bar{B} = (3) + (1 - \sqrt{-5}),$$

provide interesting examples of products, namely

$$A^2 = (2), \quad AB = (1 + \sqrt{-5}), \quad A\bar{B} = (1 - \sqrt{-5}), \quad B\bar{B} = (3),$$

which may be verified in the exercises below. It follows that the two factorizations

$$6 = 2 \cdot 3, \quad 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

can finally be reconciled—by splitting them further into the single factorization of ideals

$$(6) = AB A\bar{B}.$$

Also, the ideals A, B, \bar{B} are *prime* because they are *maximal*; that is, each is properly contained only in the ideal $\mathbb{Z}[\sqrt{-5}]$ itself. The reason for considering maximal ideals to be prime is that a prime ideal P is defined as an ideal, not equal to the whole ring, with the prime divisor property:

If P divides AB then P divides A or P divides B .

Since “to divide is to contain,” an equivalent statement of this property is:

$$\text{If } P \supseteq AB \text{ then } P \supseteq A \text{ or } P \supseteq B.$$

It is easily checked, using the above definition of the product AB , that a maximal ideal P satisfies this condition.

In $\mathbb{Z}[\sqrt{-5}]$ it is quite easy to show that A, B, \bar{B} are all maximal, so

$$(6) = AB A\bar{B}$$

is a prime ideal factorization. Moreover, it can be shown to be unique.

Dedekind (1871) showed unique prime ideal factorization holds not only for the number 6 in $\mathbb{Z}[\sqrt{-5}]$ but for any algebraic integer in the ring of integers of a field of finite dimension over \mathbb{Q} .

Dedekind's breakthrough inspired Emmy Noether in the 1920s to develop a general theory of rings and ideals, which became the foundation of modern research in algebraic number theory and algebraic geometry. Noether (1926) was able to describe precisely which rings admit unique prime ideal factorization. Today they are called *Dedekind rings*.

EXERCISES

First, let us check two properties claimed above for ideals in \mathbb{Z} .

16.9.1 If $I \subseteq \mathbb{Z}$ is a nonzero ideal, use the division property in \mathbb{Z} to prove that $I = (a)$, where a is the smallest positive member of I .

16.9.2 Deduce from 16.9.1 that $(a) + (b) = (\gcd(a, b))$.

Now we turn our attention to ideals in $\mathbb{Z}[\sqrt{-5}]$.

16.9.3 Check that

$$\begin{aligned} (2) + (1 + \sqrt{-5}) &= \{2\mu + (1 + \sqrt{-5})\nu : \mu, \nu \in \mathbb{Z}[\sqrt{-5}]\} \\ &= \{2m + (1 + \sqrt{-5})n : m, n \in \mathbb{Z}\}. \end{aligned}$$

16.9.4 Letting $A = \{2m + (1 + \sqrt{-5})n : m, n \in \mathbb{Z}\}$, verify that each member of A^2 is a multiple of 2.

16.9.5 Show in turn that $1 - \sqrt{-5} \in A$, $6 \in A^2$, and $4 \in A^2$. Deduce that $2 \in A^2$ and hence that $A^2 = (2)$.

16.9.6 Letting $B = (3) + (1 + \sqrt{-5})$ and $\bar{B} = (3) + (1 - \sqrt{-5})$, show similarly that $AB = (1 + \sqrt{-5})$, $A\bar{B} = (1 - \sqrt{-5})$, and $B\bar{B} = (3)$.



17

Sets, Logic, and Computation

PREVIEW

In the 19th century, perennial concerns about the role of infinity in mathematics were finally addressed by the development of *set theory* and *formal logic*. Set theory was proposed as a mathematical theory of infinity and formal logic was proposed as a mathematical theory of proof (partly to avoid the paradoxes that seem to arise when reasoning about infinity).

In this chapter we discuss these two developments, whose interaction led to mind-bending consequences in the 20th century. Both set theory and logic throw completely new light on the question, “What is mathematics?” But they turn out to be double-edged swords.

- Set theory brings remarkable clarity to the concept of infinity, but it shows infinity to be unexpectedly complicated—in fact, more complicated than set theory itself can describe.
- Formal logic encompasses all known methods of proof, but at the same time it shows these methods to be *incomplete*. In particular, any reasonably strong system of logic cannot prove its own consistency.
- Formal logic is the origin of the concept of *computability*, which gives a rigorous definition of an *algorithmically solvable problem*. However, some important problems turn out to be *unsolvable*.

17.1 Sets

Sets became part of mathematics in the late 19th century through attempts to understand the real numbers. Our intuition of the real numbers—that they form a line without gaps—is a mystery that mathematicians have struggled to explain since ancient times. It underlies the concept of motion that Zeno tried to challenge with his paradoxes; it resurfaced with calculus in the 17th century; and it intruded into algebra when Gauss used the intermediate value theorem in his 1816 proof of the fundamental theorem of algebra. As we mentioned in Section 11.4, Bolzano (1817) realized that the intermediate value theorem demands a proof, but he did not have a concept of real number on which a proof could be soundly based.

Bolzano did, however, realize the need for a *completeness* property of \mathbb{R} that expresses the absence of gaps. He identified the *least upper bound property*, that every bounded set of real numbers has a least upper bound, and the equivalent *nested interval property*, that if

$$a_0 < a_1 < a_2 < \cdots < b_2 < b_1 < b_0$$

then there is a number x such that

$$a_0 < a_1 < a_2 < \cdots \leq x \leq \cdots < b_2 < b_1 < b_0.$$

To prove such properties, we have to answer the question, what *is* a real number? Several equivalent answers were given around 1870, all involving infinite sets or sequences. The simplest was that of Dedekind (1872), who defined a real number to be a partition (or *cut*) of the rational numbers into two sets, L and U , such that each member of L is less than all members of U . If one has a preconceived notion of real number, such as a point x on a line, then L and U are uniquely determined by x as the sets of rational points to left and right of it, respectively. Thus if x is preconceived, then L and U are no more than auxiliary concepts that enable x to be handled in terms of rationals, as Eudoxus did (Section 4.2). Dedekind's breakthrough was to realize that no preconceived x is necessary: x is *defined by* the pair (L, U) . Thus the concept of sets of rationals became a basis for the concept of real number.

Dedekind cuts give a precise model for the continuous number line \mathbb{R} , since they fill all the gaps in the rationals. Indeed, wherever there is a gap in the rationals, the object that fills it is essentially the gap itself: the pair of sets L, U to left and right of it. Other formulations of this completeness

property of \mathbb{R} are also easy consequences of Dedekind's definition. For example, each bounded set of reals (L_i, U_i) has a least upper bound (L, U) : L is simply the union of the sets L_i .

Dedekind seemed to have settled the ancient problem of explaining the continuous in terms of the discrete, but in penetrating as far as he did, he also uncovered deeper problems. The central problem is that the completeness of \mathbb{R} entails its *uncountability*, a phenomenon discovered by Cantor (1874). The *countable* sets are those that can be put in one-to-one correspondence with $\mathbb{N} = \{0, 1, 2, \dots\}$. They include the set of rationals and also the set of algebraic numbers, as Cantor learned from Dedekind. But if \mathbb{R} is countable, this means that all reals can be included in a sequence x_0, x_1, x_2, \dots . Cantor (1874) showed that this is impossible by selecting from each sequence $\{x_m\}$ of distinct reals a subsequence $a_0, b_0, a_1, b_1, a_2, b_2, \dots$, such that

$$a_0 < a_1 < a_2 < \dots < b_2 < b_1 < b_0$$

and with each x_m *outside* one of the nested intervals $(a_0, b_0) \supset (a_1, b_1) \supset (a_2, b_2) \supset \dots$. It follows that any common element of all the (a_n, b_n) is a real $x \neq$ each x_m . A common element obviously exists if the sequence of intervals is finite, and if the sequence is infinite, it exists by completeness, as the least upper bound of the a_n . The common element x is a “gap” in the given sequence $\{x_m\}$.

This method, though ingenious, is by no means the easiest way to prove that \mathbb{R} is uncountable. In Section 17.5 we will see a simpler method that Cantor discovered later. Another simple method, using the concept of measure, is in Section 17.3.

EXERCISES

Cantor's 1874 proof of the uncountability of \mathbb{R} is based on the following construction. Given a sequence x_0, x_1, x_2, \dots of distinct reals, he found a gap in them by picking out $a_0, b_0, a_1, b_1, \dots$ as follows:

$$\begin{aligned} a_0 &= x_0, \\ b_0 &= \text{first } x_m \text{ with } a_0 < x_m, \\ a_1 &= \text{first } x_m \text{ after } b_0 \text{ with } a_0 < x_m < b_0, \\ b_1 &= \text{first } x_m \text{ after } a_1 \text{ with } a_1 < x_m < b_0, \\ a_2 &= \text{first } x_m \text{ after } b_1 \text{ with } a_1 < x_m < b_1. \\ &\vdots \end{aligned}$$

- 17.1.1** Explain why the sequence $a_0, b_0, a_1, b_1, a_2, b_2, \dots$ has the gap property described above: each x_m is outside one of the nested intervals $(a_0, b_0) \supset (a_1, b_1) \supset (a_2, b_2) \supset \dots$.

We now explore how far we can enlarge the set of natural numbers and still have a countable set.

- 17.1.2** Give a rule for continuing the sequence

$$\frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{3}{1}, \frac{2}{2}, \frac{1}{3}, \frac{4}{1}, \frac{3}{2}, \dots$$

so as to include all positive rationals.

- 17.1.3** How can one then conclude that the set of all rationals is countable?
- 17.1.4** The words on a fixed finite alphabet can be enumerated by listing first the one-letter words, then the two-letter words, and so on. Use this observation to show that the set of polynomial equations with integer coefficients is countable and hence that the set of algebraic numbers is countable.

Cantor used the latter result to prove the existence of transcendental numbers. Namely, let $\{x_m\}$ be the sequence of algebraic numbers; we know that these are not all the real numbers, so any other real number is transcendental.

17.2 Ordinals

The uncountability of \mathbb{R} has been a great challenge to set theorists and logicians ever since its discovery. The most successful response to this challenge has been the theory of *ordinal numbers*. This grew out of Cantor's (1872) investigation of trigonometric series, which leads to the problem of analyzing the complexity of point sets. Cantor measured complexity by the number of iterations of the prime operation (' of taking the limit points of a set. For example, if $S = \{0, 1/2, 3/4, 7/8, \dots, 1\}$, then the prime operation can be applied once, and $S' = \{1\}$. It can happen that S' itself has limit points, so that S'' also exists. In fact, one can find a set S for which $S', S'', \dots, S^{(n)}, \dots$ exist for all finite n , so one can envisage iterating the prime operation an infinite number of times. In the case where all the $S^{(n)}$ exist, Cantor (1880) took their intersection, thereby defining

$$S^\infty = \cap_{n=1,2,3,\dots} S^{(n)}.$$

He viewed ∞ as the first infinite ordinal number. To avoid confusion with higher infinite numbers soon to appear, I will use the modern notation ω for the first infinite ordinal.

Having made the leap to ω , it is easy to go further: $(S^{(\omega)})' = S^{(\omega+1)}$, $(S^{(\omega+1)})' = S^{(\omega+2)}$, \dots , and the intersection of this new infinite sequence is $S^{\omega \cdot 2}$, where $\omega \cdot 2$ is the first infinite number after ω , $\omega + 1$, $\omega + 2$, \dots . After $\omega \cdot 2$, one has

$$\omega \cdot 2 + 1, \omega \cdot 2 + 2, \dots, \omega \cdot 3, \dots, \omega \cdot 4, \dots, \dots, \omega \cdot \omega, \dots$$

All these ordinal numbers can actually be realized as numbers of iterations of the prime operation on sets of reals. We can also investigate the ordinal numbers independently of this realization, as an extension of the concept of natural number.

Cantor (1883) viewed the ordinals as the result of two operations:

- (i) Successor, which for each ordinal α gives the next ordinal, $\alpha + 1$.
- (ii) Least upper bound, which for each set $\{\alpha_i\}$ of ordinals gives the least ordinal \geq each α_i .

The most elegant formalization of these notions was given by von Neumann (1923). The empty set \emptyset (not considered by Cantor) is taken to be the ordinal 0, the successor of α is $\alpha \cup \{\alpha\}$, and the least upper bound of $\{\alpha_i\}$ is simply the union of the α_i . Thus

$$\begin{aligned} 0 &= \emptyset, \\ 1 &= \{0\}, \\ 2 &= \{0, 1\}, \\ &\dots \\ \omega &= \{0, 1, 2, \dots, n, \dots\}, \\ \omega + 1 &= \{0, 1, 2, \dots, n, \dots, \omega\}, \end{aligned}$$

and so on. The natural ordering of the ordinals is then given by set membership, \in , and, in particular, the members of an ordinal α are all ordinals smaller than α .

Cantor's principle (ii) generates ordinals of breathtaking size, since it gives the power to transcend any set of ordinals already defined. In particular, an ordinal of *uncountable* size is on the horizon as soon as one thinks of the concept of countable ordinal, as Cantor did (1883). He defined an ordinal α to be countable (or, as he later put it, of *cardinality* or cardinal

number \aleph_0) if α could be put in one-to-one correspondence with \mathbb{N} . For example,

$$\omega \cdot 2 = \{0, 1, 2, \dots, \omega, \omega + 1, \omega + 2, \dots\}$$

is countable because of its obvious correspondence with

$$\mathbb{N} = \{0, 2, 4, \dots, 1, 3, 5, \dots\}.$$

The least upper bound of the countable ordinals is the least *uncountable* ordinal, ω_1 . Sets in one-to-one correspondence with ω_1 are of the next cardinality, \aleph_1 . Ordinals of cardinality \aleph_1 have a least upper bound ω_2 of cardinality \aleph_2 , and so on. (\aleph is *aleph*, the first letter of the Hebrew alphabet.)

Having found this orderly way of generating successive uncountable cardinals, Cantor reconsidered the uncountable set \mathbb{R} . Although no method of generating members of \mathbb{R} in the manner of ordinals was apparent, Cantor conjectured that the cardinality of \mathbb{R} was \aleph_1 . This conjecture has since become known as the *continuum hypothesis*. By 1900 it was recognized as the outstanding open problem of set theory, and Hilbert (1900a) made it number one on the famous list of problems he presented to the mathematical community. There have been two outstanding results on the continuum problem since 1900, but together they seem to make it harder to know whether the continuum hypothesis is true. Gödel (1938) showed that the continuum hypothesis is *consistent* with standard axioms for set theory, but Cohen (1963) showed that its negation is also consistent. Thus the continuum hypothesis is independent of standard set theory, in the same way that the parallel postulate is independent of Euclid's other postulates. Whether this means that the notion of "set" is open to different natural interpretations, like the notion of "straight line," is not yet clear.

EXERCISES

For each countable ordinal α there is a set of rationals in $[0,1]$ with *order type* α . For example, the set $\{0, 1/2, 3/4, 7/8, \dots\}$ has order type ω .

- 17.2.1** Give an example of a set of rationals in $[0,1]$ with order type $\omega \cdot 2$.
- 17.2.2** Give an example of a set of rationals in $[0,1]$ with order type $\omega \cdot \omega$.
- 17.2.3** Given sets of rationals in $[0,1]$ with order types $\alpha_1, \alpha_2, \alpha_3, \dots$, explain how to obtain a set of rationals in $[0,1]$ with order type at least as large as the least upper bound of $\{\alpha_1, \alpha_2, \alpha_3, \dots\}$.
- 17.2.4** Explain why there is a set of rationals in $[0,1]$, with order type α , for each countable ordinal α .

17.3 Measure

Cantor's reason for investigating sets of discontinuities in the theory of trigonometric series goes back to the discovery of Fourier (1822) that these series depend on integrals. Assuming that

$$f(x) = \frac{1}{2}a_0 + \sum_{n=1}^{\infty} (a_n \cos n\pi x + b_n \sin n\pi x),$$

Fourier derived the formulas

$$a_n = \int_{-1}^1 f(x) \cos n\pi x \, dx, \quad b_n = \int_{-1}^1 f(x) \sin n\pi x \, dx.$$

Thus the existence of the series depends on the existence of the integrals for a_n and b_n , and this in turn depends on how discontinuous f is. It was known (though not rigorously proved) that every continuous function has an integral, so the next question was how the integral should, or could, be defined for discontinuous functions. The first precise answer was the Riemann (1854a) integral concept, familiar to all calculus students, and based on approximating the integrand by step functions. Any bounded function with a finite number of discontinuities has a Riemann integral, and indeed so have certain functions with infinitely many discontinuities, but not all. The classic function for which the Riemann integral does not exist is the function of Dirichlet (1829):

$$f(x) = \begin{cases} 1 & \text{if } x \text{ is rational,} \\ 0 & \text{if } x \text{ is irrational.} \end{cases}$$

Eventually a more general integral, the Lebesgue integral, was introduced to cope with such functions, but not until the focus of attention had shifted from the problem of integration to the more fundamental problem of *measure*. Measure generalizes the concept of length (on the line \mathbb{R}), area (in the plane \mathbb{R}^2), and so on, to quite general point sets. Since an integral can be viewed as the area under a graph, its dependence on the concept of measure is clear, though it was not immediately realized that the measure of sets on the line had to be clarified first.

The need for clarification arose from the discovery of Harnack (1885) that any countable subset $\{x_0, x_1, x_2, \dots\}$ of \mathbb{R} could be covered by a collection of intervals of arbitrarily small total length. Namely, cover x_0 by

an interval of length $\varepsilon/2$, x_1 by an interval of length $\varepsilon/4$, x_2 by an interval of length $\varepsilon/8$, \dots , so that the total length of intervals used is $\leq \varepsilon$. (This is another proof, by the way, that \mathbb{R} is *not* a countable set.) This seemed to show that countable sets were “small”—of *measure zero*, as we now say—but mathematicians were reluctant to say this of dense countable sets, like the rationals. The first response, by Jordan (1892), was to define measure analogously to the Riemann integral, using finite unions of intervals to approximate subsets of \mathbb{R} . Under this definition, “sparse” countable sets like $\{0, 1/2, 3/4, 7/8, \dots\}$ did have measure zero, but dense sets like the rationals were not measurable at all.

The first to take the hint from Harnack’s result that countable unions of intervals should be used to measure subsets of \mathbb{R} was Borel (1898). He defined the measure of any interval to be its length, and he extended measurability to more and more complicated sets by *complementation* and *countable disjoint unions*. That is, if a set S contained in an interval I has measure $\mu(S)$, then

$$\mu(I - S) = \mu(I) - \mu(S),$$

and if S is a disjoint union of sets S_n with measures $\mu(S_n)$, then

$$\mu(S) = \sum_{n=1}^{\infty} \mu(S_n).$$

The sets that can be formed from intervals by complementation and countable unions are now called *Borel sets*. Borel’s idea was pushed to its logical conclusion by Lebesgue (1902), who assigned measure zero to any subset of a Borel set of measure zero. Since not all such sets are Borel, this extended measurability to a larger class of sets: those that differ from Borel’s by sets of measure zero. It can be proved that the class of Lebesgue measurable sets has the same cardinality as the class of all subsets of \mathbb{R} . But whether the measurable sets *are* all subsets of \mathbb{R} is an interesting question to which we return shortly.

The distinctive property of Borel–Lebesgue measure is *countable additivity*: if S_0, S_1, S_2, \dots are disjoint measurable sets, then

$$\mu(S_0 \cup S_1 \cup S_2 \cup \dots) = \mu(S_0) + \mu(S_1) + \mu(S_2) + \dots.$$

This follows easily from Borel’s definition of measure for countable disjoint unions, because any countable union can be reassembled as a countable disjoint union.

Lebesgue showed that countable additivity gives a concept of integral that is better behaved with respect to limits than the Riemann integral. For example, one has the *monotone convergence property*: if f_0, f_1, f_2, \dots is an increasing sequence of positive integrable functions, and $f_n \rightarrow f$ as $n \rightarrow \infty$, then $\int f_n dx \rightarrow \int f dx$ for the Lebesgue integral, whereas this is not generally true for the Riemann integral (see Exercise 17.3.1).

It could be said that set theory paved the way for measure theory by showing the uncountability of \mathbb{R} , thus enabling countable subsets of \mathbb{R} to be regarded as “small.” On the other hand, measure theory itself shows the uncountability of \mathbb{R} (by Harnack’s result), and in fact measure theory’s assessment of the smallness of countable sets greatly influenced the later development of set theory.

“Measure theoretically desirable” axioms, such as the measurability of all subsets of \mathbb{R} , turned out to conflict with “set theoretically desirable” axioms such as the continuum hypothesis, and efforts to resolve the conflict brought to light more fundamental questions about sets. These questions do not reduce to clear-cut alternatives—the way geometric questions reduce to alternative parallel axioms, for example—but they do seem to gravitate toward the *choice* and *large cardinal* axioms, discussed in the next section.

EXERCISES

17.3.1 Show that a function f_n that is zero at all but n points has Riemann integral zero over any interval and that the non-Riemann integrable function of Dirichlet is a limit as $n \rightarrow \infty$ of such functions f_n .

The complexity of Borel sets may be roughly measured by the number of countable unions and complements needed to define them. Here are a few of the simpler ones.

17.3.2 Show that a single point is the complement of a countable union of intervals and hence that any countable set is a Borel set.

17.3.3 Deduce that the set of irrational numbers is a Borel set.

17.3.4 What is the measure of the set of irrationals between 0 and 1?

17.4 Axiom of Choice and Large Cardinals

In its usual formulation, the axiom of choice states that any set S (of nonempty sets) has a *choice function* f such that $f(x) \in x$ for each $x \in S$.

(Thus f “chooses” an element from each set x in S .) The axiom seems so plausible that early set theorists used it almost unconsciously, and it first attracted attention in Zermelo’s (1904) proof that any set S could be *well ordered* (that is, put in one-to-one correspondence with an ordinal). This looked like progress toward the continuum hypothesis. But Zermelo’s proof gave no more than the existence of a well-ordering of S , given a choice function for the set of subsets of S . There was still no sign of an explicit well-ordering of \mathbb{R} . And of course if one doubted the existence of a well-ordering of \mathbb{R} , this threw doubt on the axiom of choice. Further doubts were raised when the axiom of choice was found to have incredible consequences in measure theory.

The first of these, discovered by Vitali (1905), was that the circle can be decomposed into countably many disjoint congruent sets. Since congruent sets have the same Lebesgue measure, it easily follows that the sets in question are not Lebesgue measurable (by countable additivity; see Exercises 17.4.2–17.4.4).

Even more paradoxical decompositions were given by Hausdorff (1914) (for the sphere) and Banach and Tarski (1924) (for the ball). The Banach–Tarski theorem states that the unit ball can be decomposed into finitely many sets that, when rigidly moved in space, form *two* unit balls! This shows that not all subsets of the ball are measurable, even if one asks only for finite, rather than countable, additivity. For an excellent discussion of the paradoxical decompositions and their connections with other parts of mathematics, see Wagon (1985).

The measure-theoretic consequences of the paradoxical decompositions follow from the geometrically natural assumption that congruent sets have the same measure. If one drops this assumption and asks only for countable additivity and nontriviality (that is, not all subsets have measure zero), then the conflict with the axiom of choice seems to disappear. No contradiction has yet been derived from these assumptions, but Ulam (1930) showed that any set possessing such a measure must be extraordinarily large—as large, in fact, as a model of set theory itself, and in particular larger than the cardinals $\aleph_1, \aleph_2, \dots, \aleph_\omega, \dots$. Thus if \mathbb{R} has a nontrivial countably additive measure, then \mathbb{R} must be far larger than \aleph_1 , and we still have a conflict with the continuum hypothesis. (For more on the “largeness” of models, see Section 17.8.)

A more desirable axiom than mere measurability would be Lebesgue measurability of all subsets of \mathbb{R} . This conflicts with the axiom of choice,

by Vitali's theorem, but it was nevertheless shown to be consistent with the usual axioms of set theory by Solovay (1970), assuming the existence of a large cardinal. Shelah (1984) showed that the large cardinal assumption is necessary.

Thus measurability of all subsets of \mathbb{R} is intimately connected with the existence of sets large enough to model the whole of set theory. This mind-boggling concept seems to be the answer to many fundamental questions. We will find ourselves drawn to it again in the next sections when we explore the influence of set theory on logic. Meanwhile, for a longer introduction to set theory, its history, and interactions with analysis, see Stillwell (2013). For recent developments in the theory of large cardinals, which some believe will throw new light on the continuum hypothesis, see Kanamori (1994) and Woodin (1999).

EXERCISES

The axiom of choice turns up even in elementary analysis, when one attempts to formalize the idea of a continuous function. A natural definition in terms of infinite sequences is equivalent to the standard ε - δ definition only if we assume the axiom of choice.

Call f *sequentially continuous* at a if, for any sequence $\{a_n\}$ such that $a_n \rightarrow a$, we have $f(a_n) \rightarrow f(a)$.

- 17.4.1** Show, assuming the axiom of choice, that if f is not continuous at a then f is not sequentially continuous at a . (It is a consequence of Cohen (1966), p. 138, that this result *cannot* be proved without the axiom of choice. It turns on the fact that countably many choices are required to prove that an infinite set contains a countable subset. The next exercise involves *uncountably* many choices.)

Vitali's decomposition of the circle is created as follows. For each θ between 0 and 2π let $S(\theta)$ be the set of points on the unit circle whose angle differs from θ by a rational multiple of 2π . Thus $S(\theta) = S(\phi)$ if $\theta - \phi = 2\pi \times$ a rational, and $S(\theta) \cap S(\phi) = \emptyset$ otherwise.

- 17.4.2** Let S be a set (existing by virtue of the axiom of choice) that contains exactly one element from each distinct $S(\theta)$ and let

$$S + 2\pi r = \{\theta + 2\pi r : \theta \in S\} \quad \text{for each rational } r.$$

(Thus $S + 2\pi r$ is S rotated through the rational multiple $2\pi r$ of 2π .) Show that any two of the sets $S + 2\pi r$ are either identical or disjoint.

- 17.4.3** Show that the circle is a countable union of sets $S + 2\pi r$.
- 17.4.4** Show that both assumptions $\mu(S) = 0$ and $\mu(S) > 0$ lead to contradictions, and hence conclude that S is nonmeasurable.

17.5 The Diagonal Argument

The uncountability of \mathbb{R} was shown again in a strikingly simple way by Cantor (1891). His argument applies most directly to the set $2^{\mathbb{N}}$ of all subsets of \mathbb{N} , but there are variants that work similarly on the set $\mathbb{N}^{\mathbb{N}}$ of integer functions and on \mathbb{R} (which can be identified with a set of integer functions in various ways). To show that there are uncountably many subsets of \mathbb{N} one shows that any countable collection S_0, S_1, S_2, \dots of sets $S_n \subseteq \mathbb{N}$ is incomplete, by constructing a new set S , different from each S_n . S is the *diagonal set* $\{n : n \notin S_n\}$, which obviously differs from S_n with respect to the number n . Q.E.D.

The “diagonal” nature of S can be seen by visualizing a table of 0’s and 1’s in which

$$m\text{th entry in } n\text{th row} = \begin{cases} 0 & \text{if } m \notin S_n, \\ 1 & \text{if } m \in S_n. \end{cases}$$

In other words, the n th row consists of the values of the characteristic function of S_n . The characteristic function of S is simply the diagonal of the table, with all values reversed. A sequence x_0, x_1, x_2, \dots of real numbers can be diagonalized similarly by forming the table whose n th row consists of the decimal digits of x_n . A suitable way to “reverse” the digits on the diagonal is to change any 1 to a 2 and any other digit to a 1. (The resulting sequence of 1’s and 2’s, after a decimal point, then defines a real number x whose decimal expansion is unique. Hence x is not just different from each x_n in its decimal expansion but is definitely a different number.)

More generally, for any table of rows of integers, that is, any sequence of integer functions f_n , one can construct an integer function f unequal to each f_n by changing the values along the diagonal of the table. The diagonal argument was in fact first given in this context, by du Bois-Reymond (1875), in order to construct an f with a greater rate of growth than all functions in a sequence f_0, f_1, f_2, \dots (Exercise 17.5.1). With hindsight, one can even see a diagonal construction in Cantor’s first (1874) argument for the uncountability of \mathbb{R} (Exercise 17.5.2).

The diagonal argument is important in set theory because it readily generalizes to show that every set has more subsets than elements (Exercise 17.5.3), and hence that there is no largest set. What was not noticed at first is that the diagonal argument also has consequences at a more concrete level. This is because the diagonal of a table is *computable* if the table as a whole is computable. Hence the argument does not merely show how

to add a new function f to a list f_0, f_1, f_2, \dots —it shows how to add a new computable function to a computable list. In other words, it is *impossible to compute a list of all computable functions*. And of course the same goes for lists of computable real numbers. This remarkable result went unnoticed in the early days of the diagonal argument because computability was not then regarded as an interesting concept, or indeed as a mathematical concept at all. The controversies over the axiom of choice, however, helped to sharpen awareness of the difference between constructive and nonconstructive functions. In the 1920s logicians began to investigate the concept of computability more seriously, and by a “kind of miracle,” as Gödel (1946) later expressed it, computability turned out to be a mathematically precise notion.

EXERCISES

The diagonal construction is quite a natural way to construct a function or real number “larger” than the members of a given countable set.

17.5.1 Given integer functions f_0, f_1, f_2, \dots , define an integer function f such that $f(m)/f_n(m) \rightarrow \infty$ as $m \rightarrow \infty$, for each n . *Hint:* Arrange that $f(m) \geq n f_n(m)$ for all $m \geq n$.

17.5.2 Show that if $a_0 < a_1 < a_2 < \dots$ is a bounded sequence of real numbers, then $a = \text{least upper bound of } \{a_0, a_1, a_2, \dots\}$ is a diagonal number of the sequence in the following sense. There are integers $k_0 < k_1 < k_2 < \dots$ such that the decimal digits of a exceed those of a_n after the k_n th place.

The last exercise applies the diagonal construction to *any* set I , to show that I has more subsets than members, so *there is no largest set*.

17.5.3 Let I be any set, and let $\{S_i\}$ be a collection of subsets of I in one-to-one correspondence with the elements i of I . Show that the natural diagonal set S of this collection is a subset of I unequal to each S_i .

17.6 Computability

The notion of computability was first formalized by Turing (1936) and Post (1936), who arrived independently at a definition of computing machine, now called a *Turing machine*. A Turing machine M is given by two finite sets, $\{q_0, q_1, \dots, q_m\}$ of *internal states* and $\{s_0, s_1, \dots, s_n\}$ of *symbols*, and a *transition function* T that formalizes the behavior of M for pairs (q_i, s_j) . The machine M is visualized as having an infinite tape, divided into squares, each of which can carry one of the symbols s_j . (For most pur-

poses, M is assumed to start on a tape with all but finitely many squares blank: s_0 is taken to denote the blank symbol.) Depending on its internal state q_i , M will make a *transition*: changing s_j to s_k , then moving one square right or left and going into a new state q_l . Thus the transition function is given by finitely many equations

$$T(q_i, s_j) = (m, s_k, q_l),$$

where $m = \pm 1$ indicates a move to right or left.

To use M to compute a function $f : \mathbb{N} \rightarrow \mathbb{N}$, we need to adopt some convention for inputs (arguments of f) and outputs (values of f). The simplest is shown in Figure 17.1. M starts in state q_0 on the leftmost 1 of a block of n 1s, on an otherwise blank tape, and halts on the leftmost 1 of a block of $f(n)$ 1s, on an otherwise blank tape. M halts by virtue of entering a *halting state*, that is, a state q_h for which M has no transition from the pair $(q_h, 1)$. A *computable function* f is one that can be represented in this way by a Turing machine M .

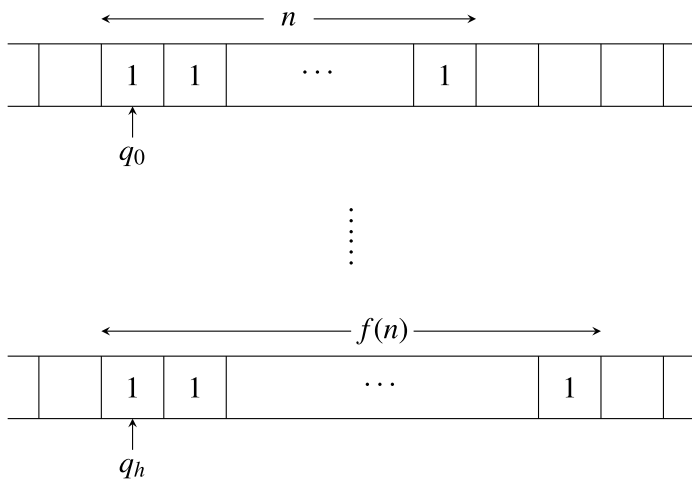


Figure 17.1: Computing a function by Turing machine

It follows that there are only countably many computable functions $f : \mathbb{N} \rightarrow \mathbb{N}$, since there are only countably many Turing machines. In fact, we can compute a list of all Turing machines by first listing the finitely many machines with one transition, then those with two transitions, and so forth. This may seem to contradict the discovery from the previous section that a

list of all computable functions cannot be computed, but, as Turing (1936) realized, it does not. The catch is that not all machines define functions, and *it is impossible to pick out all of those that do*. Of course, it is possible to rule out any machine that halts in a situation unlike that in Figure 17.1; the difficulty is in knowing whether halting is going to occur at all. It is precisely this difficulty that prevents computation of the diagonal function.

If it could be decided, for each machine M and each input, whether M eventually halts, then we could find the first machine to halt on input 1, the next after that to halt on input 2, the next after that to halt on input 3, and so on. By changing the corresponding outputs according to some rule (say, adding 1 if the output is a number, and taking the value 1 otherwise), we could compute a function different from each computable function.

This contradiction shows that the problem of deciding, given a machine and an input, whether halting eventually occurs, is *unsolvable*. This problem is called the *halting problem* and its unsolvability means that no Turing machine can solve it. That is, if the questions “Does M on input n eventually halt?” are written in some fixed finite alphabet, then there is no machine that, given these questions as inputs, will give their answers as outputs. The point is that, as far as we know, all possible rules or algorithms for answering infinite sets of questions can be realized by Turing machines. This is the “kind of miracle” referred to by Gödel (1946).

Now that computers are everywhere, it is taken for granted that the word “computability” has a precise, absolute meaning—synonymous with Turing machine computability. It is even a familiar fact that all computations can be done on a single, sufficiently powerful machine; this corresponds to the discovery of Turing (1936) of a *universal Turing machine*. However, these claims were surprising in the 1930s, particularly to Gödel, who had shown (1931) that the related notion of “provability” is *not* absolute. This will be discussed further in the next section. Briefly, the reason for the difference is that new computable functions cannot be created by diagonalization, whereas new theorems can.

Unsolvable Problems

The halting problem was of no obvious mathematical significance in 1936, but it seemed no more difficult than other unsolved algorithmic problems in mathematics. Thus for the first time it was reasonable to suspect that some ordinary mathematical problems were unsolvable. Moreover, if it

could be shown that a solution of a particular problem P implied a solution of the halting problem, then the unsolvability of P would be rigorously established. This method was used to demonstrate the unsolvability of some problems in formal logic by Turing (1936) and Church (1936). Church (1938) also put forward a strong candidate for unsolvability in ordinary mathematics: the word problem for groups.

This is the problem of deciding, given a finite set of defining relations for a group G (Section 14.7) and a word w , whether $w = 1$ in G . There is more than a superficial analogy between the word problem and the halting problem. The group G corresponds to a machine M , words in G correspond to expressions on M 's tape, and $w = 1$ corresponds to halting. The defining relations of G roughly correspond to the transition function of M , but unfortunately there is no machine equivalent of the cancellation of inverses in G . This creates fierce technical difficulties, but they were overcome by Novikov (1955). He succeeded in establishing the validity of the analogy and hence the unsolvability of the word problem. This led to unsolvability results for a host of significant mathematical problems, among them the homeomorphism problem mentioned in Section 15.5 (The reference given there, Stillwell (1993), also includes a proof of the unsolvability of the word problem.)

EXERCISES

Turing (1936) actually discovered the unsolvability of the halting problem by considering computable *real numbers* and applying the diagonal argument to them. The argument is similar to the one above using computable functions, but a little messier. Define a real number x to be *computable* if there is a Turing machine M that represents x in the following manner.

- Starting on a blank tape, M prints the decimal digits of x on successive squares of tape, eventually filling each square to the right of the square initially scanned (if necessary, printing all 0s beyond a certain point).
- The squares to the left may be used, and reused, for preliminary computation, but squares to the right, once written, may not be rewritten.

- 17.6.1** Show that there is no algorithm for recognizing the Turing machines that define real numbers in this way, since such an algorithm would give a way to compute a number different from every computable number.
- 17.6.2** Explain informally how each Turing machine M may be converted to a machine M' such that M defines a computable number if and only if M' does not halt.
- 17.6.3** Hence prove that no Turing machine can solve the halting problem.

17.7 Logic and Gödel's Theorem

Since the time of Leibniz, and perhaps earlier, attempts have been made to mechanize mathematical reasoning. There was little success until the late 19th century, when reduction of the many concepts of number, space, function, and the like, to the single concept of set simplified the axioms that seemed to be necessary for mathematics. At about the same time, investigation of the principles of logic by Boole (1847), and particularly Frege (1879), led to a system of rules by which all logical consequences of a given set of axioms could be derived. These two lines of investigation together offered the possibility of a complete, rigorous, and, in principle, *mechanical* system for deriving all mathematics.

The *Principia Mathematica* of Whitehead and Russell (1910) was a massive attempt to realize this possibility. *Principia* used axioms about sets, together with simple rules of inference, to derive a large part of ordinary mathematics in a completely formal language. When Whitehead and Russell began writing the *Principia* in 1900, they believed that they were about to reach the 19th-century goal of completeness and absolute rigor. They did not know that the rigor of their system—the ability to check proofs mechanically—was in fact *incompatible* with completeness. Gödel (1931) found true sentences expressible in the language of *Principia* that do not follow from its axioms. (Unless *Principia* is inconsistent, in which case all sentences follow and the system is useless.)

Gödel's theorem created a sensation when it first appeared. It shattered previous conceptions of mathematics and logic, and its proof was of a new and bewildering kind. Gödel exploited the mechanical nature of proof in *Principia* to define the relation “the n th sentence of *Principia* is provable” in the language of *Principia* itself. Using this, he was able to concoct a sentence that says, in effect, “This sentence is not provable.” The Gödel sentence, if true, is therefore not provable. And if false, it is provable, and so *Principia* proves a false sentence. Either way, provability in *Principia* is not the same as truth.

Gödel's proof was very difficult for his contemporaries to understand. Along with the novelty of treating sentences and proofs as mathematical objects was the near inconsistency of a sentence expressing its own unprovability (a sentence that says “This sentence is not true” is inconsistent). Post (1944) presented Gödel's theorem less paradoxically, and tied it to computability theory, by using the classical diagonal argument.

Post's Approach to Gödel's Theorem

The key to Post's approach is the concept of a *computably enumerable set* (called *recursively enumerable* in Post's time). A set W is computably enumerable if a list of its members can be computed, say by a Turing machine that prints them on its tape. (Of course if W is infinite, the computation runs forever.) A typical computably enumerable set is the set of theorems of a formal system, such as *Principia Mathematica*. For such a system one can list all sentences, then all finite sequences of sentences, and then, by picking out those sequences that are proofs, make a list of all theorems—since a theorem is simply the last line of a proof.

Post's idea was to look at the theorems about computably enumerable sets proved in a given system Σ and to compute a “diagonal sentence” from them. Since computably enumerable sets are associated with Turing machines, it is possible to enumerate the computably enumerable subsets of \mathbb{N} as W_0, W_1, W_2, \dots by letting W_n be the set of numbers output by the n th machine, under some reasonable convention. (Incidentally, there is no problem of picking out suitable machines, as there is for computable functions, since we do not mind if W_n is empty.) The diagonal set

$$D = \{n : n \notin W_n\},$$

being unequal to each W_n , is of course not computably enumerable, but the following set is:

$$\text{Pr}(D) = \{n : \Sigma \text{ proves } “n \notin W_n”\}.$$

This “provable part” of D is computably enumerable because we can list the theorems of Σ and select those of the form “ $n \notin W_n$.” Assuming that Σ proves only correct sentences we have $\text{Pr}(D) \subseteq D$, but $\text{Pr}(D) \neq D$ since $\text{Pr}(D)$ is computably enumerable and D is not. This shows immediately that there is an n_0 in D that is not in $\text{Pr}(D)$, that is, an $n_0 \notin W_{n_0}$ for which “ $n_0 \notin W_{n_0}$ ” is not provable.

Better still, a *specific* n_0 with this property is the index of the computably enumerable set $\text{Pr}(D)$. If $W_{n_0} = \text{Pr}(D)$, then $n_0 \in W_{n_0}$ is equivalent to $n_0 \in \text{Pr}(D)$, which means that “ $n_0 \notin W_{n_0}$ ” is provable. But then it is true that $n_0 \notin W_{n_0}$, assuming that Σ proves only correct sentences, and we have a contradiction. Thus $n_0 \notin W_{n_0}$. This in turn is equivalent to $n_0 \notin \text{Pr}(D)$, which means “ $n_0 \notin W_{n_0}$ ” is not provable. (Notice, incidentally, that the last part of this argument reveals “ $n_0 \notin W_{n_0}$ ” to be a sentence that expresses its own unprovability.)

Post was aware of this approach to Gödel's theorem in the 1920s, before Gödel's own proof appeared. However, Post's more general view of incompleteness as a property of arbitrary computably enumerable systems held him up until he was satisfied that computability was a mathematically definable concept. In December 1925 Post formulated a plan for proving *Principia Mathematica* incomplete but, as he later wrote, "The plan, however, included prior calisthenics at other mathematical and logical work, and did not count on the appearance of a Gödel!" (Post (1941), p. 418).

The Unprovability of Consistency

Gödel's theorem comes from reflecting on the nature of proofs. An even more devastating theorem, known as Gödel's second theorem, comes from reflecting on the proof of Gödel's theorem itself. The latter proof, unusual though it is, can be expressed in ordinary mathematical language.

We described Post's proof of Gödel's theorem in an informal language of Turing machines. But with some effort it can be expressed in the system for number theory called *Peano arithmetic* (PA), mentioned in Section 3.3. Indeed, this *arithmetization of syntax* was one of Gödel's greatest ideas. By doing his proof in PA, he exposed the incompleteness of classical mathematics. Turing machines can be discussed in PA by encoding sequences of symbols on the tape as numerals, so that machine operations become operations on numbers. Under this encoding, " $n_0 \notin W_{n_0}$ " and " Σ does not prove ' $n_0 \notin W_{n_0}$ '" become sentences of PA.

Here it is important to recall the assumption about Σ used to prove Gödel's theorem: Σ proves only correct sentences. This assumption cannot be dropped (since a false sentence implies *all* sentences), but it can be weakened to the assumption that Σ does not prove the sentence " $0 = 1$." The latter assumption says that a certain number (the number of the sentence " $0 = 1$ ") is not in a certain computably enumerable set (the set of theorems of Σ), so it can be expressed as a sentence of PA, call it $\text{Con}(\Sigma)$. In particular, PA expresses its own consistency by the sentence $\text{Con}(\text{PA})$. Gödel's theorem for $\Sigma = \text{PA}$ then becomes the following sentence of PA:

$$\text{Con}(\text{PA}) \Rightarrow \text{PA does not prove } "n_0 \notin W_{n_0}."$$

As we know, the sentence " $n_0 \notin W_{n_0}$ " is equivalent to its own unprovability, so an equivalent of the last sentence is simply

$$\text{Con}(\text{PA}) \Rightarrow n_0 \notin W_{n_0}.$$

Now Gödel noticed that his *proof* could be carried out in PA. This happened after some prompting from von Neumann (1930), who noticed the same thing. (The rather laborious verification was carried out by Hilbert and Bernays (1939)). Consequently, if $\text{Con}(\text{PA})$ can be proved in PA, then so can “ $n_0 \notin W_{n_0}$,” by basic logic. But if PA is consistent, “ $n_0 \notin W_{n_0}$ ” *cannot* be proved in it, by Gödel’s theorem, hence neither can $\text{Con}(\text{PA})$. (Gödel of course had a different unprovable sentence, but it was similarly implied by $\text{Con}(\text{PA})$, and equivalent to its own unprovability.)

Thus the assertion $\text{Con}(\text{PA})$ that the axioms of PA are consistent is in some way stronger than the axioms themselves. Similarly, if Σ is any system that includes PA (such as *Principia Mathematica* and other systems of set theory), then $\text{Con}(\Sigma)$ cannot be proved in Σ , if Σ is consistent. This is Gödel’s second theorem.

EXERCISES

It is instructive to spell out why the sentence “ $n_0 \notin W_{n_0}$ ” expresses its own unprovability, if this is not already obvious.

17.7.1 Fill in the gap so as to establish a chain of equivalences:

$$n_0 \notin W_{n_0} \Leftrightarrow \cdots \Leftrightarrow \Sigma \text{ does not prove “} n_0 \notin W_{n_0} \text{”}.$$

A remarkable new form of Gödel’s theorem was discovered by Chaitin (1970). Like Gödel’s own version, it is most easily explained in terms of computation. Let us call a finite sequence σ of 0s and 1s *computationally random* if it cannot be produced (from a blank tape) by a Turing machine whose description is shorter than σ . To compare lengths fairly we assume that Turing machines are themselves written as sequences of 0s and 1s. (This makes the definition of “computationally random” dependent on the way we encode Turing machines, but never mind—the proof of Chaitin’s theorem assumes only that the method of encoding is computable.)

17.7.2 Give an informal argument to explain why the sequence of 10^{100} consecutive 0s is *not* computationally random.

17.7.3 Show that at most $2^n - 1$ Turing machines have descriptions of length less than n .

17.7.4 Deduce from Exercise 17.7.3 that there are infinitely many computationally random sequences.

Despite the prevalence of computationally random sequences, they are very hard to find. Chaitin’s incompleteness theorem states: *any sound formal system proves only finitely many theorems of the form “ σ is computationally random.”*

To prove Chaitin's theorem suppose, on the contrary, that there is a formal system, and hence a Turing machine M , that generates infinitely many theorems of the form “ σ is computationally random,” and no false statements of this form. Suppose, for example, that M has length 10^6 .

17.7.5 Explain informally how to convert M to a machine M' that finds the first theorem of the form “ σ is computationally random” output by M , where σ has at least 10^{100} digits.

17.7.6 Also explain informally why the length of M' is less than 10^{100} .

17.7.7 Deduce from Exercise 17.7.6 that we have a contradiction; hence M does not exist.

17.8 Provability and Truth

The previous section stressed that Gödel's theorem is a statement of alternatives: a formal system Σ either fails to prove a true sentence or else proves a false one. Gödel's second theorem identifies a sentence, $\text{Con}(\Sigma)$, which is either true and unprovable or false and provable, but does not say which alternative holds for a particular Σ , such as PA or *Principia*. How could it, without violating Gödel's theorem itself? Unless Σ actually is *inconsistent*, there can be no proof in Σ that $\text{Con}(\Sigma)$ is true!

Nevertheless, Gödel's theorem tells us that we have nothing to lose by adding $\text{Con}(\Sigma)$ to the system Σ . If Σ is inconsistent, then it is already worthless, and we are no worse off for having added $\text{Con}(\Sigma)$. And if Σ is consistent, we actually gain, because $\text{Con}(\Sigma)$ is a new mathematical truth not provable from Σ alone. In this way, Gödel's theorem allows us to transcend any given formal system. Knowing that $\text{Con}(\Sigma)$ is beyond the scope of Σ (if Σ is consistent) is of practical value to mathematicians, for it means there is no point trying to prove any sentence that implies $\text{Con}(\Sigma)$. If one wants to use such a sentence, it should be taken as a new axiom.

Sentences of mathematical interest actually arise in this way, most simply in set theory, where consistency is implied by the existence of a “large set.” The usual axioms of set theory (called the Zermelo–Fraenkel, or ZF, axioms) say roughly that

(i) \mathbb{N} is a set.

(ii) Further sets result from certain operations, the most important of which are *power* (taking all subsets of a set) and *replacement* (taking the range of a function whose domain is a set).

Because of this, the axioms of ZF can be modeled by any set that contains \mathbb{N} and is closed under power and replacement. Such a set has to be very large—larger than any set whose existence can be proved in ZF—but if it exists then ZF must be consistent, since two contradictory sentences cannot be true of an actually existing object. Thus the existence of a set that is large in the above sense implies $\text{Con}(\text{ZF})$.

If ZF is consistent, then $\text{ZF} + \text{Con}(\text{ZF})$ is also consistent, but an even larger set is required to satisfy the enlarged axiom system. These large-set existence axioms are called *axioms of infinity*. Since they imply $\text{Con}(\text{ZF})$, they cannot be proved in ZF. In particular, one cannot prove the existence of a nontrivial measure on all subsets of \mathbb{R} since, as mentioned in Section 17.3, this implies the existence of a large set. Gödel (1946) made the interesting speculation that any true but unprovable proposition is a consequence of some axiom of infinity.

More recently, some largeness properties in number theory have been found to imply $\text{Con}(\text{PA})$. The first of these was found by Paris and Harrington (1977), using a modification of a combinatorial theorem of Ramsey (1929). Paris and Harrington found a sentence σ that says that for each $n \in \mathbb{N}$ there is an m such that sets of size $\geq m$ have a certain combinatorial property $C(n)$. They showed that σ follows from a well-known theorem on infinite sets, called *Ramsey's theorem*, but that the function

$$f(n) = \text{least } m \text{ such that sets of size } m \text{ have property } C(n)$$

grows faster than any computable function whose existence can be proved in PA. Thus σ in some sense asserts the existence of a large function. The property $C(n)$ is such that one can decide whether a finite set has it or not; hence σ implies (very simply, and certainly in PA) that f is computable. This shows immediately that σ cannot be proved in PA, but Paris and Harrington in fact proved the stronger result that σ implies $\text{Con}(\text{PA})$. For an excellent introduction to Ramsey theory and the Paris-Harrington theorem, see Katz and Reimann (2018).

Gödel's theorem shows that something is missing in the formal view of mathematics, and the axioms of infinity show that the missing elements may be mathematically interesting and important. Despite this, it is commonly thought that mathematics consists in the formal deduction of theorems from fixed axioms. As early as 1941 Post protested against this view:

It is to the writer's continuing amazement that ten years after Gödel's remarkable achievement current views on the nature

of mathematics are thereby affected only to the point of seeing the need of many formal systems, instead of a universal one. Rather has it seemed to us to be inevitable that these developments will result in a reversal of the entire axiomatic trend of the late 19th and early 20th centuries, with a return to meaning and truth.

Post (1941), p. 345

Things have indeed not turned out as Post expected—the “axiomatic trend” rolls on—but there has been a “reversal” of sorts. The last 40 years have seen the development of *reverse mathematics*, the aim of which is to find the “right” axioms to prove given theorems, in the sense given by the seminal work of Friedman (1975):

When a theorem is proved from the right axioms, the axioms can be proved from the theorem.

For example, Euclid’s parallel axiom is the right axiom to prove the theorem of Pythagoras, the theorem that the angle sum of a triangle is π , and many other geometric theorems, because it can be shown that these theorems imply the parallel axiom. More precisely, the parallel axiom can be proved from them assuming only the *other* axioms of Euclid. These implications were known long ago, but they became interesting only when Beltrami (1868a) showed that the parallel axiom is *not* provable from Euclid’s other axioms. Thus a reverse mathematics of Euclidean geometry becomes possible with the discovery that the parallel axiom is independent of Euclid’s other axioms.

Modern reverse mathematics begins with the discoveries of Post, Turing, and Gödel that certain real numbers are not computable. From this it follows, using the relations they found between logic, computation, and arithmetic, that certain axioms about infinite sets of natural numbers are independent of basic axioms about the natural numbers. (The basics are, roughly, PA plus an axiom stating the existence of computable sets). It turns out, surprisingly, that a small number of these seemingly obscure axioms about infinity are the “right” axioms to prove standard theorems about real numbers and continuous functions.

Reverse mathematics today covers not only analysis, but also parts of topology, combinatorics, and algebra. For an introduction, see Stillwell (2018), and for a more encyclopedic treatment, see Simpson (2009).

EXERCISES

An argument for the unprovability of “large” sets that does not assume the unprovability of consistency was discovered by Zermelo in 1928 (Zermelo’s announcement is mentioned in Baer (1928)). Since this was before Gödel’s own work, it seems fair to call this *Zermelo’s incompleteness theorem*. It states that, if “large” sets exist, then this fact is not provable in ZF.

To pave the way for Zermelo’s argument, we need to explain how ordinals measure the “complexity level”—called the *rank*—of sets. The simplest set is the empty set 0, which is assigned rank 0. For each ordinal α , the sets of rank $\leq \alpha + 1$ are those of rank $\leq \alpha$, together with all subsets of the set of sets of rank $\leq \alpha$.

17.8.1 Show that $1 = \{0\}$ has rank 1, and more generally that $n + 1 = \{0, 1, \dots, n\}$ has rank $n + 1$.

If λ is an ordinal *not* of the form $\alpha + 1$, the sets of rank $\leq \lambda$ are those of rank $\alpha < \lambda$, together with all subsets of the set of sets of rank $< \lambda$.

17.8.2 Show that the ordinal $\omega = \{0, 1, 2, \dots\}$ has rank ω .

17.8.3 More generally, show that any ordinal α has rank α .

It is essentially an axiom of ZF (the *axiom of foundation*) that every set has a rank.

An ordinal λ is called *inaccessible* if the sets of rank $< \lambda$ are closed under the power and replacement operations. Thus, if an inaccessible λ exists, the sets of rank $< \lambda$ form a model of ZF. Also, if inaccessible ordinals exist, there is a *least* inaccessible, μ .

17.8.4 Show that the sets of rank $< \mu$ are a model of ZF plus the sentence “there is no inaccessible ordinal.”

17.8.5 Deduce from Exercise 17.8.4 that, if inaccessible ordinals exist, this fact is not provable in ZF.

For a wide-ranging introduction to the interplay between logic and infinity, see Stillwell (2010b).

Image Credits

All images are due to the author, with the exception of those listed below. Many of these classic images are now freely viewable online, so I include URLs of sites where they may be seen. In most cases the URL takes you directly to the image itself, but it will also be possible to step forward or backward from the page, to see the image in its full context. These URLs were sourced on April 10, 2020, and of course they may expire, but alternative sources will likely be found by searching for a few key words.

Figure 2.1, which was generated from POV-Ray code in Wikimedia, sourced on April 7, 2020:

<https://en.wikipedia.org/wiki/User:Cyp/Poly.pov>

Figure 2.3, from Kepler (1596), between pages 24 and 25.

<https://www.e-rara.ch/zut/content/zoom/123244>

Figure 5.2, from Zhū Shijié (1303), p. 46 of the 1937 reprint.

Figure 6.1, from Huygens (1692), p. 352.

<http://ckcc.huygens.knaw.nl/epistolarium/letter.html?id=huyg003/2777>

Figure 6.2, from Grandi (1723), after p. 371.

<https://royalsocietypublishing.org/doi/pdf/10.1098/rstl.1722.0070>

Figure 6.3, from Harris (1708), p. 214.

<https://play.google.com/books/reader?id=gUsoAQAAMAAJ&hl=en&pg=GBS.PP210>

Figure 7.1, from the British Library manuscript Yates Thompson MS 47, entitled *The Lives of Sts. Edmund and Fremund* by John Lydgate, c.1434, page f.13v.

http://www.bl.uk/manuscripts/Viewer.aspx?ref=harley_ms_2278_fs001r

Used with permission of the British Library Board, 16/5/2020.

Figure 7.2, from Dürer (1525), p. 180.

https://commons.wikimedia.org/wiki/Category:Underweysung_der_Messung#/media/File:Duerer_Underweysung_der_Messung_180.jpg

Figure 7.6, from Leonardo da Vinci, *Codex Atlanticus*, c. 1500, folio 98r.
<http://www.codex-atlanticus.it/#/Detail?detail=98>

Figure 7.7, which consists of two images from Wikimedia, sourced on April 5, 2020, both in the public domain:

[https://en.wikipedia.org/wiki/The_Ambassadors_\(Holbein\)#/media/File:Hans_Holbein_the_Younger_-_The_Ambassadors_-_Google_Art_Project.jpg](https://en.wikipedia.org/wiki/The_Ambassadors_(Holbein)#/media/File:Hans_Holbein_the_Younger_-_The_Ambassadors_-_Google_Art_Project.jpg)

https://commons.wikimedia.org/wiki/File:Holbein_Skull.jpg

The first image is a part of the former file. The second image is by Thomas Shahan, released by him into the public domain.

Figure 7.8, from Nicéron (1638), p. 134.

https://archive.org/details/BIUSante_01737/page/n171/mode/2up

Figure 11.1, from a 1569 version of Bombelli, *L'Algebra*, p. 72 verso of Codice B. 1569 in the Biblioteca comunale dell' Archiginnasio, Bologna. Used with their permission.

Figure 13.15, from Klein (1928), p. 286.

[https://gdz.sub.uni-goettingen.de/id/PPN375534636?tify=%22pages%22:\[298\],%22view%22:%22info%22](https://gdz.sub.uni-goettingen.de/id/PPN375534636?tify=%22pages%22:[298],%22view%22:%22info%22)

Reprinted by permission from Springer Nature Customer Service Centre GmbH: Springer *Vorlesungen über Nicht-Euklidische Geometrie* by Felix Klein, copyright 1928.

Figure 15.7, which is a grayscale version of an image by Anton Sherwood from Wikimedia, in the public domain:

https://en.wikipedia.org/wiki/Uniform_tilings_in_hyperbolic_plane#/media/File:H2_tiling-288-1.png

Bibliography

Abel NH (1826) Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré. *J reine und angew Math* 1:65–84. *Oeuvres Complètes* 1:66–87

Abel NH (1827) Recherches sur les fonctions elliptiques. *J reine und angew Math* 2:101–181. 3:160–190. In his *Oeuvres Complètes* 1:263–388

Abel NH (1829) Mémoire sur une classe particulière d'équations résolubles algébriquement. *J reine und angew Math* 4:131–156. *Œuvres Complètes* 1:478–507

Adyan SI (1957) Unsolvability of some algorithmic problems in the theory of groups (Russian). *Trudy Moskov Mat Obshch* 6:231–298

Alberti LB (1436) *Trattato della pittura*. Reprinted in *Il trattato della pittura e i cinque ordine architetonici*, R. Carabba, 1913

Apéry R (1981) Interpolation de fractions continues et irrationalité de certaines constantes. In: *Mathematics, CTHS: Bull. Sec. Sci., III*, pp 37–53. *Bib. Nat., Paris*

Argand JR (1806) *Essai sur une manière de représenter les quantités imaginaires dans les constructions géométriques.*, Paris

Ayoub R (1984) The lemniscate and Fagnano's contributions to elliptic integrals. *Arch Hist Exact Sci* 29(2):131–149

Bachet de Méziriac CG (1621) *Diophanti Alexandrini libri sex*. Toulouse

Baer R (1928) Zur Axiomatik der Kardinalarithmetik. *Math Zeit* 29:381–396

Ball WWR (1890) Newton's classification of cubic curves. *Proc London Math Soc* 22:104–143

Baltrušaitis J (1977) *Anamorphic art*. Harry Abrams, New York

© Springer Nature Switzerland AG 2020

J. Stillwell, *Mathematics and Its History*, Undergraduate Texts in Mathematics,

<https://doi.org/10.1007/978-3-030-55193-3>

- Banach S, Tarski A (1924) Sur la décomposition des ensembles de points en parties respectivement congruentes. *Fund Math* 6:244–277
- Baron ME (1969) The origins of the infinitesimal calculus. Pergamon Press, Oxford
- Bashmakova IG (1981) Arithmetic of algebraic curves from Diophantus to Poincaré. *Historia Math* 8(4):393–416
- Beeckman I (1628) Journal. Beeckman (1634), quoted in *Œuvres de Descartes*, vol 10, pp 344–346
- Beeckman I (1634) Journal tenu par Isaac Beeckman de 1604 à 1634. Nijhoff, The Hague. Edited by C. de Waard, 4 vols
- Beltrami E (1865) Risoluzione del problema: Riportare i punti di una superficie sopra un piano in modo che le linee geodetiche vengano rappresentate da linee rette. *Ann Mat pura appl*, ser 1 7:185–204. In his *Opere Matematiche* 1:262–280
- Beltrami E (1868a) Saggio di interpretazione della geometria non-euclidea. *Giorn Mat* 6:284–312. In his *Opere Matematiche* 1:262–280, English translation in Stillwell (1996)
- Beltrami E (1868b) Teoria fondamentale degli spazii di curvatura costante. *Ann Mat pura appl*, ser 2 2:232–255. In his *Opere Matematiche* 1:406–429, English translation in Stillwell (1996)
- Bernoulli J (1692) Lineae cycloides, evolutae, ant-evolutae ... Spira mirabilis. *Acta Erud* 11:207–213
- Bernoulli J (1694) Curvatura laminae elasticae. *Acta Erud* 13:262–276
- Bernoulli J, Johann (1704) Über unendliche Reihen. *Ostwald's Klassiker*, vol 171. Engelmann, Leipzig, 1909
- Bernoulli J (1691) Solutio problematis funicularii. *Acta Erud* 10:274–276. In his *Opera Omnia* 1:48–51
- Bernoulli J (1702) Solution d'un problème concernant le calcul intégral, avec quelques abrégés par rapport à ce calcul. *Mém Acad Roy Soc Paris*, 289–297. In his *Opera Omnia* 1:393–400
- Bernoulli J (1712) Angulorum arcuumque sectio indefinita. *Acta Erud* 31:274–277. In his *Opera Omnia* 1:511–514

- Bézout E (1779) *Théorie générale des équations algébriques*. Paris, Ph.-D. Pierres. English translation: *General Theory of Algebraic Equations*, by Eric Feron, Princeton University Press, Princeton, 2006
- Birkhoff G (ed) (1973) *A source book in classical analysis*. Harvard University Press, Cambridge, MA, With the assistance of Uta Merzbach
- Boltyansky VG (1978) *Hilbert's third problem*. V. H. Winston & Sons, Washington, DC. Translated from the Russian by Richard A. Silverman, with a foreword by Albert B. J. Novikoff, Scripta Series in Mathematics
- Bolyai F (1832a) *Tentamen juventutem studiosam in elementa matheseos purae, elementaris ac sublimioris, methodo intuitiva, evidentiaque huic propria, introducendi*. Marosvásárhely
- Bolyai J (1832b) *Scientiam spatii absolute veram exhibens: a veritate aut falsitate Axiomatis XI Euclidei (a priori haud unquam decidanda) independentem*. Appendix to Bolyai (1832a), English translation in Bonola (1912)
- Bolzano B (1817) *Rein analytischer Beweis des Lehrsatzes dass zwischen je zwey Werthen, die ein entgegengesetztes Resultat gewähren, wenigstens eine reelle Wurzel der Gleichung liege*. Ostwald's Klassiker, vol 153. Engelmann, Leipzig, 1905. English translation in Russ (2004), pp 251–277
- Bombelli R (1572) *L'algebra*. Prima edizione integrale. Introduzione di U. Forti. Prefazione di E. Bortolotti. Reprint by Biblioteca scientifica Feltrinelli. 13. Milano: Giangiacomo Feltrinelli Editore. LXIII (1966)
- Bonnet O (1848) *Mémoire sur la théorie générale des surfaces*. J Éc Polytech 19:1–146
- Bonola R (1912) *Noneuclidean geometry*. Open Court, Chicago. Reprinted by Dover, New York, 1955
- Boole G (1847) *Mathematical analysis of logic*. Reprinted by Basil Blackwell, London, 1948
- Borel E (1898) *Leçons sur la théorie des fonctions*. Gauthier-Villars, Paris
- Bos HJM (1981) On the representation of curves in Descartes' *Géométrie*. Arch Hist Exact Sci 24(4):295–338
- Bos HJM (1984) Arguments on motivation in the rise and decline of a mathematical theory; the "construction of equations," 1637–ca. 1750. Arch Hist Exact Sci 30(3-4):331–380
- Bosse A (1648) *Manière universelle de Mr Desargues*. P. Des-Hayes, Paris

- Bourgne R, Azra J-P (1962) *Ecrits et mémoires mathématiques d'Évariste Galois: Édition critique intégrale de ses manuscrits et publications*. Gauthier-Villars & Cie, Imprimeur-Éditeur-Libraire, Paris. Préface de J. Dieudonné
- Boyer CB (1956) *History of analytic geometry*. Scripta Mathematica, New York
- Boyer CB (1959) *The history of the calculus and its conceptual development*. Dover Publications Inc, New York
- Boyer CB (1968) *A history of mathematics*. Wiley, New York
- Brahana HR (1921) Systems of circuits on 2-dimensional manifolds. *Ann Math* 23:144–168
- Brahmagupta (628) *Brâhma-sphuṭa-siddhânta*. Partial English translation in Colebrooke (1817)
- Bressoud DM (2019) *Calculus reordered*. Princeton University Press, Princeton and Oxford
- Brieskorn E, Knörrer H (1981) *Ebene algebraische Kurven*. Birkhäuser Verlag, Basel. English translation: *Plane algebraic curves*, by John Stillwell, Birkhäuser Verlag, 1986
- Briggs H (1624) *Arithmetica logarithmica*. William Jones, London
- Bring ES (1786) *Meletemata quaedam mathematica circa transformationem aequationum algebraicarum*. Lund University. Promotionschrift
- Burton DM (1985) *The history of mathematics*. Allyn and Bacon Inc, Boston, MA
- Cajori F (1913) History of the exponential and logarithmic concepts. *Am Math Monthly* 20:5–14, 35–47, 75–84, 107–117, 148–151, 173–182, 205–210
- Cantor G (1872) Über die Ausdehnung eines Satzes aus der Theorie der trigonometrischen Reihen. *Math Ann* 5:123–132. In his *Gesammelte Abhandlungen*, 92–102
- Cantor G (1874) Über eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen. *J reine und angew Math* 77:258–262. In his *Gesammelte Abhandlungen*, 145–148. English translation by W. Ewald in Ewald (1996), vol II, pp 840–843
- Cantor G (1880) Über unendlich lineare Punktmannigfaltigkeiten, 2. *Math Ann* 17:355–358. In his *Gesammelte Abhandlungen*, 145–148

- Cantor G (1883) Grundlagen einer allgemeinen Mannigfaltigkeitslehre. Teubner, Leipzig. In his *Gesammelte Abhandlungen*, 165–204. English translation by W. Ewald in Ewald (1996), vol II, pp 878–919
- Cantor G (1891) Über eine elementare Frage der Mannigfaltigkeitslehre. *Jahresber deutsch Math Verein* 1:75–78. English translation by W. Ewald in Ewald (1996), vol II, pp 920–922
- Cardano G (1545) *Ars magna*. 1968 translation *The great art or the rules of algebra* by T. Richard Witmer, with a foreword by Oystein Ore. The M.I.T. Press, Cambridge, MA-London
- Cauchy A-L (1813) Démonstration du théorème général de Fermat sur les nombres polygones. *Mém Sci Math Phys Inst France*, ser 1 14:177–220. In his *Œuvres*, ser 2, 6:320–353
- Cauchy A-L (1815) Mémoire sur le nombre des valeurs qu’une fonction peut acquérir, lorsqu’on y permute de toutes les manières possibles les quantités qu’elle renferme. *J Éc Polytech* 18:1–28. In his *Œuvres*, ser 2, 1:62–90
- Cauchy A-L (1825) Mémoire sur les intégrales définies prises entre des limites imaginaires. Paris
- Cauchy A-L (1837) Letter to Coriolis, 29 January 1837. *Comp Rend* 4:214–218. In his *Œuvres*, ser 1, 4:38–42
- Cauchy A-L (1844) Mémoire sur les arrangements que l’on peut former avec des lettres données, et sur les permutations ou substitutions à l’aide desquelles on passe d’un arrangement à un autre. *Ex anal phys math* 3:151–252. In his *Œuvres*, ser 2, 13:171–282
- Cauchy A-L (1846) Sur les intégrales qui s’étendent à tous les points d’une courbe fermée. *Comp Rend* 23:251–255. In his *Œuvres*, ser 1, 10:70–74
- Cauchy A-L (1847) Mémoire sur le théorie des équivalences algébriques, substituée à la théorie des imaginaires, pp 87–110. In his *Exercices d’analyse et de physique mathématique*, Tome 4
- Cavalieri B (1635) *Geometria indivisibilibus continuorum nova quadam ratione promota*. Clement Ferroni, Bononi
- Cayley A (1854) On the theory of groups, as depending on the symbolic equation $\theta^n = 1$. *Phil Mag* 7:40–47. In his *Collected Mathematical Papers* 2:123–130
- Cayley A (1859) A sixth memoir on quantics. *Phil Trans Roy Soc* 149:61–90. In his *Collected Mathematical Papers* 2:561–592

- Cayley A (1878) The theory of groups. *Am J Math* 1:50–52. In his *Collected Mathematical Papers* 10:401–403
- Chaitin GJ (1970) Computational complexity and Gödel's incompleteness theorem. *Not Am Math Soc* 17:672
- Chandler B, Magnus W (1982) *The history of combinatorial group theory*. Springer, New York
- Church A (1936) An unsolvable problem in elementary number theory. *Am J Math* 58:345–363
- Church A (1938) *Rev J Symb Logic* 3:46
- Clagett M (1968) *Nicole Oresme and the medieval geometry of qualities and motions*. University of Wisconsin Press, Madison
- Clay M, Margalit D (eds) (2017) *Office hours with a geometric group theorist*. Princeton University Press, Princeton, NJ
- Clebsch A (1864) Über einen Satz von Steiner und einige Punkte der Theorie der Curven dritter Ordnung. *J reine und angew Math* 63:94–121
- Cohen P (1963) The independence of the continuum hypothesis I, II. *Proc Nat Acad Sci* 50, 51:1143–1148, 105–110
- Cohen PJ (1966) *Set theory and the continuum hypothesis*. W. A. Benjamin Inc, New York-Amsterdam
- Colebrooke HT (1817) *Algebra, with Arithmetic and Mensuration, from the Sanscrit of Brahme Gupta and Bhāscara*. John Murray, London. Reprinted by Martin Sandig, Wiesbaden, 1973
- Cotes R (1714) *Logometria*. *Phil Trans* 29:5–45
- Cotes R (1722) *Harmonia mensurarum*. Robert Smith, Cambridge
- Cox DA (1984) The arithmetic-geometric mean of Gauss. *Enseign Math* (2) 30(3–4):275–330
- Cramer G (1750) *Introduction à l'analyse des lignes courbes algébriques*. Geneva
- Crossley JN (1987) *The emergence of number*, 2nd edn. World Scientific Publishing Co., Singapore
- d'Alembert JLR (1746) *Recherches sur le calcul intégral*. *Hist Acad Sci Berlin* 2:182–224

- d'Alembert JLR (1752) *Essai d'une nouvelle théorie de la résistance des fluides*. David, Paris
- Davenport JH (1981) *On the integration of algebraic functions*. Springer, Berlin
- Davis M (ed) (1965) *The Undecidable. Basic papers on undecidable propositions, unsolvable problems and computable functions*. Raven Press, Hewlett, NY
- Davis M (1973) Hilbert's tenth problem is unsolvable. *Am Math Monthly* 80:233–269
- de Moivre A (1698) A method of extracting the root of an infinite equation. *Phil Trans* 20:190–193
- de Moivre A (1707) *Æquationem quarundum potestatis tertiae, quintae septimae, nonae & superiorum, ad infinitum usque pergendo, in terminis finitis, ad instar regularum pro cubicis que vocantur Cardani, resolutio analytica*. *Phil Trans* 25:2368–2371
- de Moivre A (1730) *Miscellanea analytica de seriebus et quadraturis*. J. Tonson and J. Watts, London
- Dedekind R (1871) Supplement X. In *Dirichlet's Vorlesungen über Zahlentheorie*, 2nd edn., Vieweg 1871
- Dedekind R (1872) *Stetigkeit und irrationale Zahlen*. Vieweg und Sohn, Braunschweig. English translation in: *Essays on the Theory of Numbers*. Dover, New York, 1963
- Dedekind R (1877) *Theory of algebraic integers*. Cambridge University Press, Cambridge. Translated from the 1877 French original and with an introduction by John Stillwell
- Dedekind R (1894) Supplement XI. In *Dirichlet's Vorlesungen über Zahlentheorie*, 4th edn., Vieweg 1894
- Dedekind R, Weber H (1882) *Theorie der algebraischen Functionen einer Veränderlichen*. *Journal für die reine und angewandte Mathematik* 92:181–291. English translation in *Dedekind and Weber* (2012)
- Dedekind R, Weber H (2012) *Theory of algebraic functions of one variable. History of mathematics, vol 39*. American Mathematical Society, Providence, RI; London Mathematical Society, London. Translated from the 1882 German original and with an introduction, bibliography and index by John Stillwell
- Dehn M (1900) Über raumgleiche Polyeder. *Gött Nachr* 1900:345–354

- Dehn M (1910) Über die Topologie des dreidimensionalen Raumes. *Math Ann* 69:137–168
- Dehn M (1912) Über unendliche diskontinuierliche Gruppen. *Math Ann* 71:116–144
- Dehn M, Heegaard P (1907) Analysis situs. *Enzyklopädie der Mathematischen Wissenschaften*, vol IIAB3, pp 153–220, Teubner, Leipzig
- Desargues G (1639) Brouillon projet d'une atteinte aux événements des rencontres du cône avec un plan. In Taton (1951), pp 99–180
- Descartes R (1637) The geometry of René Descartes. (With a facsimile of the first edition, 1637.). Dover Publications Inc, New York, NY. Translated by David Eugene Smith and Marcia L. Latham, 1954
- Descartes R (1638) Letter to Mersenne, 18 January 1638. *Œuvres* 1:490
- Dickson LE (1903) Introduction to the theory of algebraic equations. Wiley, New York
- Dickson LE (1920) History of the theory of numbers. Vol. II: diophantine analysis. Chelsea Publishing Co, New York. 1966 reprint of Carnegie Institute, Washington, edition
- Dirichlet PGL (1829) Sur la convergence des séries trigonométriques qui servent à représenter une fonction arbitraire entre des limites données. *J reine und angew Math* 4:157–169. In his *Werke* 1:117–132
- Dombrowski P (1979) 150 Years after Gauss' "Disquisitiones generales circa superficies curvas". Société Mathématique de France, Paris. With the original text of Gauss
- du Bois-Reymond P (1875) Über asymptotische Werte, infinitäre Approximationen und infinitäre Auflösung von Gleichungen. *Math Ann* 8:363–414
- du Bois-Reymond P (1875) Über asymptotische Werte, infinitäre Approximationen und infinitäre Auflösung von Gleichungen. *Math Ann* 8:363–414
- Dyck W (1882) Gruppentheoretische Studien. *Math Ann* 20:1–44
- Dyck W (1883) Gruppentheoretische Studien II. *Math Ann* 22:70–108
- Edwards CH Jr (1979) The historical development of the calculus. Springer, New York
- Edwards HM (1974) Riemann's zeta function. Academic Press, New York-London, *Pure and applied mathematics*, vol 58

Edwards HM (1984) Galois theory. Springer, New York

Edwards HM (2007) Kronecker's fundamental theorem of general arithmetic. In: Episodes in the history of modern algebra (1800–1950), pp 107–116. American Mathematical Society, Providence, RI

Eisenstein G (1847) Beiträge zur Theorie der elliptische Functionen. J reine und angew Math 35:137–274

Eisenstein G (1850) Über einige allgemeine Eigenschaften der Gleichung, von welcher die Theorie der ganzen Lemniscate abhängt. J reine und angew Math 39:556–619

Euler L (1728a) De linea brevissima in superficie quacunque duo quaelibet puncta iungente. Comm Acad Sci Petrop 3:110–124. In his Opera Omnia, series 1, 25:1–12

Euler L (1728b) Letter to John Bernoulli, 10 December 1728. Bibl Math, ser 3, 4:352–354

Euler L (1734) De summis serierum reciprocarum. Comm Acad Sci Petrop 7. In his Opera Omnia, ser 1, 14:73–86

Euler L (1736) Theorematum quorundam ad numeros primos spectantium demonstratio. Comm Acad Sci Petrop 8:141–146. In his Opera Omnia, ser 1, 2:33–37

Euler L (1746) Letter to Goldbach, 14 June 1746. Briefwechsel Opera Omnia, ser quarta A, 1:52

Euler L (1746) Letter to Goldbach, 14 June 1746. Briefwechsel Opera Omnia, ser quarta A, 1:52

Euler L (1748b) Introductio in analysin infinitorum, II. Volume 9 of his Opera Omnia, series 1. English translation, Introduction to the analysis of the infinite. Book II. Springer, 1988

Euler L (1750) Letter to Goldbach, 9 June 1750. In Fuss (1968), I:521–524

Euler L (1752) Elementa doctrinae solidorum. Novi Comm Acad Sci Petrop 4:109–140. In his Opera Omnia, ser 1, 26:71–93

Euler L (1758) Theoremata arithmetica nova methodo demonstrata. Novi Comm Acad Sci Petrop 8:74–104. In his Opera Omnia, ser 1, 2:531–555

Euler L (1760) Recherches sur la courbure des surfaces. Mém Acad Sci Berlin 16:119–143. In his Opera Omnia, ser 1, 28:1–22

Euler L (1768) Institutiones calculi integralis. Opera Omnia, ser 1, 11

- Euler L (1770a) De summis serierum numeros bernoullianos involventium. *Novi Comm Acad Sci Petrop* 14:129–167
- Euler L (1770b) *Elements of Algebra*. Translated from the German by John Hewlett. Reprint of the (1840) edition, with an introduction by C. Springer, New York, Truesdell, 1984
- Euler L (1777) De repraesentatione superficiei sphaericae super plano. *Acta Acad Sci Imper Petrop* 1:107–132
- Euler L (1849) De numeris amicabilebus. *Comm Arith* 2:627–636. In his *Opera Omnia*, ser 1, 5:353–365
- Ewald W (1996) *From Kant to Hilbert: a source book in the foundations of mathematics*, vol I, II. The Clarendon Press, Oxford University Press, New York
- Fagnano GCT (1718) Metodo per misurare la lemniscata. *Giorn lett d'Italia* 29. In his *Opere Matematiche* 2:293–313
- Fauvel J, Gray J (eds) (1988) *The history of mathematics: a reader*. Macmillan Press Ltd, Basingstoke. Reprint of the 1987 edition
- Federico PJ (1982) *Descartes on polyhedra*. Springer, New York. A study of the *De solidorum elementis*
- Fermat P (1629) Ad locos planos et solidos isagoge. *Œuvres* 1:92–103. English translation in Smith (1959), 389–396
- Fermat P (1640) Letter to Frenicle, 18 October 1640. *Œuvres* 2:209
- Fermat P (1670) Observations sur Diophante. *Œuvres* 3:241–276
- Fibonacci (1225) *Flos Leonardo Bigolli Pisani super solutionibus quarundam quaestionum ad numerum et ad geometriam pertinentium*
- Field JV, Gray JJ (1987) *The geometrical work of Girard Desargues*. Springer, New York
- Fourier J (1822) *La théorie analytique de la chaleur*. Didot, Paris. English translation, *The analytical theory of heat*. Dover, New York, 1955
- Fowler DH (1980) Book II of Euclid's *Elements* and a pre-Eudoxan theory of ratio. *Arch Hist Exact Sci* 22(1–2):5–36
- Fowler DH (1982) Book II of Euclid's *Elements* and a pre-Eudoxan theory of ratio. II. Sides and diameters. *Arch Hist Exact Sci* 26(3):193–209
- Frege G (1879) *Begriffsschrift*. English translation in van Heijenoort (1967)

- Friedman H (1975) Some systems of second order arithmetic and their use. In: Proceedings of the international congress of mathematicians (Vancouver, B.C., 1974), vol 1, pp 235–242. Canadian Mathematical Congress, Montreal, Quebec
- Fritsch R (1984) The transcendence of π has been known for about a century-but who was the man who discovered it? *Resultate Math* 7(2):164–183
- Fuss P-H (1968) Correspondance mathématique et physique de quelques célèbres géomètres du XVIIIème siècle. Tomes I, II. Johnson Reprint Corp, New York. Reprint of the Euler correspondence originally published by l'Académie Impériale des Sciences de Saint-Pétersbourg. The Sources of Science, No. 35
- Galois E (1831a) Analyse d'un mémoire sur la résolution algébrique des équations. In Bourgne and Azra (1962), pp 163–165
- Galois E (1831b) Mémoire sur les conditions de résolubilité des équations par radicaux. In Bourgne and Azra (1962), pp 43–71
- Gauss CF (1799) Demonstratio nova theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse. Helmstedt dissertation, in his Werke 3:1–30
- Gauss CF (1801) Disquisitiones arithmeticae. Translated and with a preface by Arthur A. Clarke. Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse. Springer, New York, 1986
- Gauss CF (1811) Letter to Bessel, 18 December 1811. Briefwechsel mit F. W. Bessel, Georg Olms Verlag, Hildesheim, 1975, pp 155–160. English translation in Birkhoff (1973)
- Gauss CF (1816) Demonstratio nova altera theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse. *Comm Recentiores (Gottingae)* 3:107–142. In his Werke 3:31–56
- Gauss CF (1818) Determinatio attractionis quam in punctum quodvis positionis datae exerceret planeta si eius massa per totam orbitam ratione temporis quo singulae partes describuntur uniformiter esset dispertita. *Comm Soc Reg Sci Gottingensis Rec* 4. In his Werke 3:331–355
- Gauss CF (1819) Die Kugel. Werke 8:351–356
- Gauss CF (1822) Allgemeine Auflösung der Aufgabe; die Theile einer gegebenen Fläche so abzubilden, dass die Abbildung dem Abgebildeten in den kleinsten Theilen ähnlich wird. *Astr Abh* 3:1–30. In his Werke 4:189–216. English translation, *Phil Mag*, new ser, 4 (1828), 104–113, 206–215

- Gauss CF (1825) Die Seitenkrümmung. Werke 8:386–395
- Gauss CF (1827) *Disquisitiones generales circa superficies curvas*. Göttingen, König. Ges. Wiss. Göttingen. English translation in Dombrowski (1979)
- Gauss CF (1828) Letter to Bessel, 30 March 1828. Briefwechsel mit F. W. Bessel, Georg Olms Verlag, Hildesheim 1975:477–478
- Gauss CF (1831) Letter to Schumacher, 12 July 1831. Werke 8:215–218
- Gelfond AO (1961) *The Solution of equations in integers*. W. H. Freeman and Co, San Francisco, CA. Translated from the Russian and edited by J. B. Roberts
- Gödel K (1931) Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme. I. Monatsh Math Phys 38:173–198
- Gödel K (1938) The consistency of the axiom of choice and the generalized continuum hypothesis. Proc Nat Acad Sci 25:220–224
- Gödel K (1946) Remarks before the Princeton bicentennial conference on problems in mathematics. In Davis (1965)
- Goldstine HH (1977) *A history of numerical analysis from the 16th through the 19th century*. Springer, New York. Studies in the history of mathematics and physical sciences, vol 2
- Gomes Teixeira F (1995a) *Traité des courbes spéciales remarquables planes et gauches*. Tome I. Éditions Jacques Gabay, Paris. Translated from the Spanish, revised and augmented. Reprint of the 1908 translation
- Gomes Teixeira F (1995b) *Traité des courbes spéciales remarquables planes et gauches*. Tome II. Éditions Jacques Gabay, Paris. Translated from the Spanish, revised and augmented. Reprint of the 1909 translation
- Gomes Teixeira F (1995c) *Traité des courbes spéciales remarquables planes et gauches*. Tome III. Éditions Jacques Gabay, Paris. Reprint of the 1915 original
- Goursat E (1900) Sur la définition générale des fonctions analytiques, d'après Cauchy. Trans Am Math Soc 1:14–16
- Grandi G (1723) *Florum geometricorum manipulus*. Phil Trans 32:355–371
- Grassmann H (1844) *Die lineale Ausdehnungslehre*. Otto Wigand. Leipzig. English translation in Grassmann (1995), pp 1–312
- Grassmann H (1847) *Geometrische Analyse geknüpft an die von Leibniz gefundene Geometrische Charakteristik*. Weidmann'sche Buchhandlung. Leipzig. English translation in Grassmann (1995), pp 313–414

- Grassmann H (1861) *Lehrbuch der Arithmetik*. Enslin, Berlin
- Grassmann H (1995) *A new branch of mathematics*. Open Court Publishing Co., Chicago, IL. The *Ausdehnungslehre* of 1844 and other works, Translated from the German and with a note by Lloyd C. Kannenberg. With a foreword by Albert C. Lewis
- Gray J (1982) From the history of a simple group. *Math Intell* 4(2):59–67
- Gray J (2018) *A history of abstract algebra*. Springer undergraduate mathematics series. Springer, Cham. From algebraic equations to modern algebra
- Green G (1828) An essay on the application of mathematical analysis to the theories of electricity and magnetism. In his *Papers* 1–115
- Gregory J (1670) Letter to Collins, 23 November 1670. In Turnbull (1939), pp 118–133
- Hadamard J (1954) *An essay on the psychology of invention in the mathematical field*. Dover Publications Inc, New York
- Hall Jr M (1967) *Combinatorial theory*. Blaisdell Publishing Co. Ginn and Co., Waltham, MA–Toronto, Ont.–London
- Hamilton WR (1856) Memorandum respecting a new system of roots of unity. *Phil Mag* 12:496. In his *Mathematical Papers* 3:610
- Harnack A (1885) Über den Inhalt von Punktmengen. *Math Ann* 25:241–250
- Harnack A (1885) Über den Inhalt von Punktmengen. *Math Ann* 25:241–250
- Hausdorff F (1914) *Grundzüge der Mengenlehre*. Von Veit, Leipzig
- Heath TL (1910) *Diophantus of Alexandria: a study in the history of Greek Algebra*. Dover Publications Inc, New York. 1964 reprint of the Cambridge University Press 2nd ed
- Heath TL (1921) *A history of Greek mathematics*. Clarendon Press, Oxford, Reprinted by Dover, New York, 1981
- Heath TL (1925) *The thirteen books of Euclid's elements*. Cambridge University Press, Cambridge, Reprinted by Dover, New York, 1956
- Hermite C (1858) Sur la résolution de l'équation du cinquième degré. *Comp Rend* 46:508–515. In his *Œuvres* 2:5–12
- Hermite C (1873) Sur la fonction exponentielle. *C. R. LXXVII*. 18–24, 74–49, 226–233, 285–293. In his *Œuvres* 3:150–181

- Hilbert D (1899) *Grundlagen der Geometrie*. Teubner, Leipzig. English translation: *Foundations of geometry*. Open Court, Chicago, 1971
- Hilbert D (1900a) *Mathematische Probleme*. Vortrag, gehalten auf dem internationalen Mathematiker-Congress zu Paris 1900. *Gött Nachr* 1900:253–297
- Hilbert D (1900b) Über das Dirichlet'sche Princip. *Jahresber Deutschen Math Ver* 8:184–188
- Hilbert D (1901) Über Flächen von constanter Gauss'scher Krümmung. *Trans Am Math Soc* 2:87–89. In his *Gesammelte Abhandlungen* 2:437–438
- Hilbert D, Bernays P (1939) *Grundlagen der Mathematik II*. Springer, Berlin
- Hilbert D, Cohn-Vossen S (1932) *Anschauliche Geometrie*. Julius Springer, Berlin. English translation: *Geometry and the imagination*. Chelsea, New York, 1952
- Hobbes T (1656) Six lessons to the professors of mathematics. *The English Works of Thomas Hobbes*, vol 7, pp 181–356, Scientia Aalen, Aalen, West Germany, 1962
- Hobbes T (1672) Considerations upon the answer of Doctor Wallis. *The English Works of Thomas Hobbes*, vol 7, pp 443–448, Scientia Aalen, Aalen, West Germany, 1962
- Hoe J (1977) Les systèmes d'équations polynômes dans le Siyuan yujian (1303) par Chu Shih-chieh. *Institut des Hautes Études Chinoises, Collège de France, Paris. Mémoires de l'Institut des Hautes Études Chinoises*, vol VI
- Hofmann JE (1974) *Leibniz in Paris, 1672–1676*. Cambridge University Press, London. His growth to mathematical maturity, Revised and translated from the German with the assistance of A. Prag and D. T. Whiteside
- Hölder O (1896) Über den Casus Irreducibilis bei der Gleichung dritten Grades. *Math Ann* 38:307–312
- Huygens C (1659) Fourth part of a treatise on quadrature. *Œuvres Complètes* 14:337
- Huygens C (1673) *Horologium oscillatorium*. In his *Œuvres Complètes* 18:69–368, English translation *The Pendulum Clock*, Iowa State University Press, Ames, IA, 1986
- Huygens C (1692) Letter to the Marquis de l'Hôpital, 29 December 1692. *Œuvres Complètes* 10:348–355

- Huygens C (1693a) Appendix to Huygens (1693b). *Œuvres Complètes* 10:481–422
- Huygens C (1693b) Letter to H. Basnage de Beauval, February 1693. *Œuvres Complètes* 10:407–417
- Jacobi CGJ (1829) *Fundamenta nova theoriae functionum ellipticarum*. Bornträger, Königsberg. In his *Werke* 1:49–239
- Jacobi CGJ (1834) De usu theoriae integralium ellipticorum et integralium abelianorum in analysi diophantea. *J reine und angew Math* 13: 353–355. In his *Werke* 2:53–55
- Jones JP, Matiyasevich YV (1991) Proof of recursive unsolvability of Hilbert's tenth problem. *Am Math Monthly* 98(8):689–709
- Jordan C (1866) Sur la déformation des surfaces. *J Math*, ser 2(11):105–109
- Jordan C (1870) *Traité des substitutions et des équations algébriques*. Éditions Jacques Gabay, Sceaux. 1989 Reprint of the 1870 original
- Jordan C (1892) Remarques sur les intégrales définies. *J Math*, ser 4(8):69–99
- Kac M (1984) How I became a mathematician. *Am Sci* 72:498–499
- Kanamori A (1994) *The higher infinite*. Springer, Berlin
- Katz M, Reimann J (2018) An introduction to Ramsey theory. Student mathematical library, vol 87. American Mathematical Society, Providence, RI; Mathematics Advanced Study Semesters, University Park, PA. Fast functions, infinity, and metamathematics
- Katz VJ, Folkerts M, Hughes B, Wagner R, Berggren JL (eds) (2016) *Sourcebook in the mathematics of medieval Europe and North Africa*. Princeton University Press, Princeton, NJ
- Katz VJ, Parshall KH (2014) *Taming the unknown*. Princeton University Press, Princeton, NJ, A history of algebra from antiquity to the early twentieth century
- Kepler J (1596) *Mysterium cosmographicum*. English translation of 1621 edition, *The Secret of the Universe*, Abaris, New York, 1981
- Kepler J (1604) *Ad vitellionem paralipomena, quibus astronomiae pars optica traditur*. Marnium & Aubrii, Frankfurt
- Kepler J (1609) *Astronomia nova*. English translation *New Astronomy*, Cambridge University Press, Cambridge, 1992

- Klein F (1871) Über die sogenannte Nicht-Euklidische Geometrie. *Math Ann* 4:573–625. In his *Gesammelte Mathematische Abhandlungen* 1: 254–305. English translation in Stillwell (1996)
- Klein F (1872) Vergleichende Betrachtungen über neuere geometrische Forschungen (Erlanger Programm). Akademische Verlagsgesellschaft. Leipzig. In his *Gesammelte Mathematischen Abhandlungen* 1:460–497
- Klein F (1874) Bemerkungen über den Zusammenhang der Flächen. *Math Ann* 7:549–557
- Klein F (1876) Über binäre Formen mit lineare Transformation in sich selbst. *Math Ann* 9:183–208. In his *Gesammelte Mathematische Abhandlungen* 2:275–301
- Klein F (1882a) Letter to Poincaré, 14 May 1882. *Gesammelte Mathematische Abhandlungen* 3:615–616
- Klein F (1882b) Neue Beiträge zur Riemannschen Funktionentheorie. *Math Ann* 21:141–218. In his *Gesammelte Mathematische Abhandlungen* 3:630–710
- Klein F (1884) Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade. Teubner, Stuttgart. Reprinted in 1993 by Birkhäuser Verlag, with an introduction and commentary by Peter Slodowy. English translation *Lectures on the Icosahedron* by Dover, 1956
- Klein F (1909) *Elementarmathematik vom höheren Standpunkte aus. Teil II: Geometrie*. B. G. Teubner, Leipzig. English translation: Klein (1939)
- Klein F (1924) *Elementarmathematik vom höheren Standpunkte aus. Erster Band: Arithmetik-Algebra-Analysis*. Springer, Berlin. English translation *Elementary mathematics from an advanced standpoint. Arithmetic-algebra-analysis*. Reprinted by Dover Publications Inc., New York, 1953
- Klein F (1928) *Vorlesungen über Nicht-Euklidische Geometrie*. Springer, Berlin
- Klein F (1939) *Elementary Mathematics from an Advanced Standpoint; Geometry*. Translated from the third German edition by E. R. Hedrick and C. A. Noble. Macmillan & Co., London
- Kline M (1972) *Mathematical thought from ancient to modern times*. Oxford University Press, New York
- Knobloch E (2013) Leibniz's theory of elimination and determinants. In: Seki, founder of modern mathematics in Japan. *Springer proceedings in mathematics and statistics*, vol 39, pp 229–244. Springer, Tokyo

- Koebe P (1907) Über die Uniformisierung beliebiger analytischer Kurven. Göttinger Nachrichten 191–210
- Kronecker L (1887) Ein Fundamentalsatz der allgemeinen Arithmetik. Journal für die reine und angewandte Mathematik 100:490–510
- Krummbiegel B, Amthor A (1880) Das Problema bovinum des Archimedes. Schlömilch Z. XXV. III. A. 121–136, 153–171
- Kummer EE (1844) De numeris complexis, qui radicibus unitatis et numeris realibus constant. Gratulationschrift der Univ. Breslau zur Jubelfeier der Univ. Königsberg. Also in Kummer (1975), vol 1, pp 165–192
- Kummer EE (1975) Collected papers. Springer, Berlin. Volume I: contributions to number theory, edited and with an introduction by André Weil
- Lagrange JL (1770) Demonstration d'un théorème d'arithmétique. Nouv Mém Acad Berlin. In his Œuvres 3:189–201
- Lagrange JL (1771) Réflexions sur la résolution algébrique des équations. Nouv Mém Acad Berlin. In his Œuvres 3:205–421
- Lagrange JL (1772) Recherches sur la manière de former des tables des planètes d'après les seules observations. Mém Acad Roy Sci Paris. In his Œuvres 6:507–627
- Lagrange JL (1779) Sur la construction des cartes géographiques. Nouv Mém Acad Berlin. In his Œuvres 4:637–692
- Lagrange JL (1785) Sur une nouvelle méthode de calcul intégral. Mém Acad Roy Soc Turin 2. In his Œuvres 2:253–312
- Lambert JH (1766) Die Theorie der Parallellinien. Mag reine und angew Math (1786) 137–164, 325–358
- Lambert JH (1772) Anmerkungen und Zusätze zur Entwerfung der Land- und Himmelscharten. English translation by Waldo R. Tobler, Michigan Geographical Publication No. 8, Department of Geography, University of Michigan, 1972
- Laurent P-A (1843) Extension du théorème de M. Cauchy relatif à la convergence du développement d'une fonction suivant les puissances ascendantes de la variable. Comp Rend 17:348–349
- Lebesgue H (1902) Intégrale, longueur, aire. Ann Mat, ser 3(7):231–359
- Legendre A-M (1794) Éléments de géométrie. F. Didot, Paris
- Legendre A-M (1825) Traité des fonctions elliptiques. Huzard-Courcier, Paris

- Leibniz GW (1675) De bisectione laterum. See Schneider (1968)
- Leibniz GW (1684) Nova methodus pro maximis et minimis. *Acta Erud* 3:467–473. In his *Mathematische Schriften* 5:220–226. English translation in Struik (1969)
- Leibniz GW (1686) De geometria recondita et analysi indivisibilium atque infinitorum. *Acta Erud* 5:292–300. Also in Leibniz's *Mathematische Schriften* 5:226–233
- Leibniz GW (1702) Specimen novum analyseos pro scientia infiniti circa summas et quadraturas. *Acta Erud* 21:210–219. In his *Mathematische Schriften* 5:350–361
- Lenstra HW (2002) Solving the Pell equation. *Not Am Math Soc* 49:182–192
- Levi ben Gershon (1321) *Maaser Hoshev*. German translation by Gerson Lange: *Sefer Maasei Choscheb*, Frankfurt 1909. English translation in Katz et al (2016)
- Li Y, Du SR (1987) *Chinese mathematics: a concise history*. The Clarendon Press, Oxford University Press, New York. Translated from the Chinese and with a preface by John N. Crossley and Anthony W.-C. Lun. With a foreword by Joseph Needham
- Lindemann F (1882) Über die Zahl π . *Math Ann* 20:213–225
- Liouville J (1833) Mémoire sur les transcendentes elliptiques de première et de seconde espèce considérées comme fonctions de leur amplitude. *J Éc Polytech* 23:37–83
- Liouville J (1850) Note IV to Monge's *Application de l'analyse à la géométrie*, 5th edn. Bachelier, Paris
- Lobachevsky NI (1829) On the foundations of geometry. *Kazansky Vestnik*. (Russian)
- Lobachevsky NI (1836) Application of imaginary geometry to some integrals. *Zap Kazan Univ* 1:3–166 (Russian)
- Lohne JA (1965) Thomas Harriot als Mathematiker. *Centaurus* 11(1):19–45
- Lohne JA (1979) Essays on Thomas Harriot. *Arch Hist Exact Sci* 20(3-4):189–312. I. Billiard balls and laws of collision, II. Ballistic parabolas, III. A survey of Harriot's scientific writings
- Maclaurin C (1720) *Geometrica organica sive descriptio linearum curvarum universalis*. G. and J. Innys, London

- Magnus W (1930) Über diskontinuierliche Gruppen mit einer definierenden Relation (der Freiheitssatz). *J reine und angew Math* 163:141–165
- Magnus W (1974) *Noneuclidean Tessellations and Their Groups*. Academic Press, New York-London. Pure and applied mathematics, vol 61
- Markov A (1958) The insolubility of the problem of homeomorphy (Russian). *Dokl Akad Nauk SSSR* 121:218–220
- Martizloff J-C (2006) *A History of Chinese mathematics* (English ed.). Springer, Berlin. With forewords by Jaques Gernet and Jean Dhombres, Translated from the 1987 French original by Stephen S. Wilson
- Matiyasevich YV (1970) The Diophantineness of enumerable sets (Russian). *Dokl Akad Nauk SSSR* 191:279–282
- McKean H, Moll V (1997) *Elliptic curves*. Cambridge University Press, Cambridge
- Melzak ZA (1976) *Companion to concrete mathematics*, vol. II. Mathematical ideas, modeling and applications. Wiley-Interscience (John Wiley & Sons), New York. Foreword by Wilhelm Magnus
- Mengoli P (1650) *Novae quadraturae arithmeticae seu de additione fractionum*. Iacob Montij, Bononi
- Mercator N (1668) *Logarithmotechnia*. William Godbid and Moses Pitt, London
- Minding F (1839) Wie sich entscheiden lässt, ob zwei gegebene krumme Flächen auf einander abwickelbar sind oder nicht; nebst Bemerkungen über die Flächen von unveränderlichem Krümmungsmasse. *J reine und angew Math* 19:370–387
- Minding F (1840) Beiträge zur Theorie der kürzesten Linien auf krummen Flächen. *J reine und angew Math* 20:323–327
- Möbius AF (1827) *Der barycentrische Calcul*. Werke 1:1–388
- Möbius AF (1863) *Theorie der Elementaren Verwandtschaft*. Werke 2:433–471
- Moise EE (1963) *Elementary geometry from an advanced standpoint*. Addison-Wesley Publishing Co., Inc, Reading, MA-Palo Alto, CA-London
- Mordell LJ (1922) On the rational solutions of the indeterminate equations of the third and fourth degrees. *Cambr Phil Soc Proc* 21:179–192
- Muir T (1960) *The theory of determinants in the historical order of development*. Dover Publications Inc, New York, Four volumes bound as two

- Nathanson MB (1987) A short proof of Cauchy's polygonal number theorem. *Proc Am Math Soc* 99(1):22–24
- Needham T (1997) *Visual complex analysis*. Clarendon Press, Oxford
- Neugebauer O, Sachs A (1945) *Mathematical cuneiform texts*. Yale University Press, New Haven, CT
- Neumann C (1870) Zur Theorie des logarithmischen und des Newtonschen Potentials, zweite Mitteilung. *Ber König Sächs Ges Wiss, math-phys Cl* 264–321
- Newton I (1665a) Annotations on Wallis. *Mathematical Papers* 1:96–111
- Newton I (1665b) The geometrical construction of equations. *Mathematical Papers* 1:492–516
- Newton I (1665c) Normals, curvature and the resolution of the general problem of tangents. *Mathematical Papers* 1:245–297
- Newton I (1667) *Enumeratio curvarum trium dimensionum*. *Mathematical Papers* 12:10–89
- Newton I (1669) *De analysi*. *Mathematical Papers* 2:206–247
- Newton I (1670s) *De resolutione quaestionum circa numeros*. *Mathematical Papers* 4:110–115
- Newton I (1671) *De methodis serierum et fluxionum*. *Mathematical Papers* 3:32–353
- Newton I (1676a) Letter to Oldenburg, 13 June 1676. In Turnbull (1960), pp 20–47
- Newton I (1676b) Letter to Oldenburg, 24 October 1676. In Turnbull (1960), pp 110–149
- Newton I (1687) *Philosophiae naturalis principia mathematica*. William Dawson & Sons, Ltd, London. Facsimile of first edition of 1687
- Newton I (1695) *Enumeratio linearum tertii ordinis*. *Mathematical Papers* 7:588–645
- Nicéron F (1638) *La perspective curieuse*. P. Billaine, Paris
- Nielsen J (1927) Untersuchungen zur Topologie der geschlossenen zweiseitigen Flächen. *Acta Math* 50:189–358
- Noether E (1926) Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern. *Mathematischen Annalen* 96:26–61

- Novikov PS (1955) On the algorithmic unsolvability of the word problem in group theory (Russian). Dokl Akad Nauk SSSR Mat Inst Tr 44. English translation in Am Math Soc Transl ser 2, 9:1–122
- Oresme N (1350a) Quaestiones super geometriam Euclidis. Edited by H. L. L. Busard. Janus, suppléments, vol III, E. J. Brill, Leiden, 1961
- Oresme N (1350b) Tractatus de configurationibus qualitatum et motuum. English translation in Clagett (1968)
- Ostrogradsky M (1828) Démonstration d’un théorème du calcul integral. Mém Acad Sci St Petersburg, ser 6(1):39–53
- Ostrowski A (1920) Über den ersten und vierten Gaußschen Beweis des Fundamentalsatzes der Algebra. Gauss Werke 10, part 2, 1–18
- Pacioli L (1509) De divina proportionem. Paganus Paganinus, Venice
- Pappus (1986) Book 7 of the Collection. Sources in the history of mathematics and physical sciences, vol 8. Springer, New York. Part 1. Introduction, text, and translation, Part 2. Commentary, index, and figures, Edited and with translation and commentary by Alexander Jones
- Paris J, Harrington L (1977) A mathematical incompleteness in Peano arithmetic. In: Barwise J (ed) Handbook of mathematical logic. North-Holland, Amsterdam
- Pascal B (1640) Essay pour les coniques. Paris
- Pascal B (1654) Traité du triangle arithmétique, avec quelques autres petits traités sur la même manière. English translation in Great Books of the Western World, Encyclopedia Britannica, London, 1952, pp 447–473
- Peano G (1889) Arithmetices principia. Bocca, Torino
- Pierpont J (1895) Zur Geschichte der Gleichung des V. Grades (bis 1858). Monatsh f Math VI:15–68
- Plofker K (2009) Mathematics in India. Princeton University Press, Princeton, NJ
- Plücker J (1830) Über ein neues Coordinatensystem. J reine angew Math 5:1–36. Gesammelte Mathematische Abhandlungen 124–158
- Poincaré H (1882) Théorie des groupes fuchsien. Acta Math 1:1–62. In his Œuvres 2:108–168. English translation in Poincaré (1985), 55–127
- Poincaré H (1883) Mémoire sur les groupes Kleinéens. Acta Math 3:49–92. English translation in Poincaré (1985), 255–304

- Poincaré H (1895) Analysis situs. J Éc Polytech, ser 2 1:1–121. In his Œuvres 6:193–288
- Poincaré H (1901) Sur les propriétés arithmétiques des courbes algébriques. J Math 7:161–233. In his Œuvres 5:483–548
- Poincaré H (1904) Cinquième complément à l'analysis situs. Palermo Rend 18:45–110. In his Œuvres 6:435–498
- Poincaré H (1907) Sur l'uniformisation des fonctions analytiques. Acta Math 31:1–63. In his Œuvres 4:70–139
- Poincaré H (1985) Papers on Fuchsian functions. Springer, New York. Translated from the French and with an introduction by John Stillwell
- Poncelet JV (1822) Traité des propriétés projectives des figures. Bachelier, Paris
- Post EL (1936) Finite combinatory processes. Formulation 1. J Symb Logic 1:103–105
- Post EL (1941) Absolutely unsolvable problems and relatively undecidable propositions. Account of an anticipation. In Davis (1965), pp 340–433
- Post EL (1944) Recursively enumerable sets of positive integers and their decision problems. Bull Am Math Soc 50:284–316
- Prouhet E (1860) Remarques sur un passage des œuvres inédits de Descartes. Comp Rend 50:779–781
- Puiseux V-A (1850) Recherches sur les fonctions algébriques. J Math 15:365–480
- Rajagopal CT, Rangachari MS (1977) On an untapped source of medieval Keralese mathematics. Arch History Exact Sci 18(2):89–102
- Rajagopal CT, Rangachari MS (1986) On medieval Kerala mathematics. Arch Hist Exact Sci 35(2):91–99
- Ramsey FP (1929) On a problem of formal logic. Proc Lond Math Soc 30:291–310
- Richeson DS (2008) Euler's Gem. Princeton University Press, Princeton
- Riemann GFB (1851) Grundlagen für eine allgemeine Theorie der Functionen einer veränderlichen complexen Grösse. Werke, 2nd edn., pp 3–48
- Riemann GFB (1854a) Über die Darstellbarkeit einer Function durch eine trigonometrische Reihe. Werke, 2nd edn., pp 227–264

- Riemann GFB (1854b) Über die Hypothesen, welche der Geometrie zu Grunde liegen. Werke, 2nd edn., pp 272–287
- Riemann GFB (1857) Theorie der Abel'schen Functionen. J reine und angew Math 54:115–155. Werke, 2nd edn., pp 82–142
- Riemann GFB (1858a) Elliptische Funktionen. Ed. H. Stahl, Leipzig, 1899
- Riemann GFB (1858b) Vorlesungen über die hypergeometrische Reihe. Werke, 2nd ed., Dover, New York, 1953
- Riemann GFB (1858b) Vorlesungen über die hypergeometrische Reihe. Werke, 2nd ed., Dover, New York, 1953
- Robert A (1973) Elliptic curves. Springer, Berlin. Notes from postgraduate lectures given in Lausanne 1971/72, Lecture notes in mathematics, vol 326
- Robinson A (1966) Non-standard analysis. North-Holland Publishing Co, Amsterdam
- Rosen M (1981) Abel's theorem on the lemniscate. Am Math Monthly 88(6):387–395
- Roy R (2011) Sources in the development of mathematics. Cambridge University Press, Cambridge, Infinite series and products from the fifteenth to the twenty-first century
- Ruffini P (1799) Teoria generale delle equazioni in cui si dimostra impossibile la soluzione algebrica delle equazioni generale di grade superiore al quarto. Bologna
- Russ S (2004) The mathematical works of Bernard Bolzano. Oxford University Press, Oxford
- Russ S (2004) The mathematical works of Bernard Bolzano. Oxford University Press, Oxford
- Salmon G (1851) Théorèmes sur les courbes de troisième degré. J reine und angew Math 42:274–276
- Schneider I (1968) Der Mathematiker Abraham de Moivre (1667–1754). Arch Hist Exact Sci 5:177–317
- Schooten Fv (1659) Geometria à Renato Des Cartes. Louis and Daniel Elzevir, Amsterdam
- Schwarz HA (1870) Über einen Grenzübergang durch alternirendes verfahren. Vierteljahrsh. Natur Ges Zürich 15:272–286. In his Mathematische Abhandlungen 2:133–143

- Schwarz HA (1872) Über diejenigen Fälle, in welchen die Gaussische hypergeometrische Reihe eine algebraische Function ihres vierten Elementes darstellt. *J reine und angew Math* 75:292–335. In his *Mathematische Abhandlungen* 2:211–259
- Seifert H, Threlfall W (1934) *Lehrbuch der Topologie*. Teubner, Leipzig. English translation *A textbook of topology*. Academic Press, New York, 1980
- Serre J-P (2003) *Trees*. Springer monographs in mathematics. Springer, Berlin. Translated from the French original by John Stillwell, Corrected 2nd printing of the 1980 English translation
- Shelah S (1984) Can you take Solovay's inaccessible away? *Israel J Math* 48(1):1–47
- Shen K-S, Crossley JN, Lun W-C (1999) *The nine chapters on the mathematical art. Companion and commentary*. Oxford University Press, Oxford
- Siegel CL (1969) *Topics in complex function theory*. Vol. I: elliptic functions and uniformization theory. Wiley-Interscience (a Division of John Wiley & Sons), New York-London-Sydney. Translated from the original German by A. Shenitzer and D. Solitar. Interscience Tracts in Pure and Applied Mathematics, no. 25
- Simpson SG (2009) *Subsystems of second order arithmetic* (2nd edn.). *Perspectives in logic*. Cambridge University Press, Cambridge; Association for Symbolic Logic, Poughkeepsie, NY
- Sluse RF (1673) A method of drawing tangents to all geometrical curves. *Phil Trans* 7:5143–5147
- Smith DE (1959) *A source book in mathematics*. Dover Publications Inc, New York, 2 vols
- Solovay RM (1970) A model of set-theory in which every set of reals is Lebesgue measurable. *Ann Math* 2(92):1–56
- Stäckel P (1901) Die Entdeckung der nichteuklidischen Geometrie durch Johann Bolyai. *Mat-natur ber Ungarn Budapest* 17:1–19
- Sternberg S (1969) *Celestial mechanics*. Part I. W. A. Benjamin, Inc, New York-Amsterdam. Mathematics lecture note series: XXII
- Stillwell J (1982) The word problem and the isomorphism problem for groups. *Bull Am Math Soc (NS)* 6:33–56
- Stillwell J (1993) *Classical topology and combinatorial group theory*, 2nd edn. Springer, New York, NY

- Stillwell J (1996) Sources of hyperbolic geometry. American Mathematical Society, Providence, RI
- Stillwell J (2005) The four pillars of geometry. Springer, New York
- Stillwell J (2010a) Mathematics and its history, 3rd edn. Undergraduate texts in mathematics, Springer, New York
- Stillwell J (2010b) Roads to infinity. A K Peters Ltd, Natick, MA
- Stillwell J (2013). The real numbers. Undergraduate texts in mathematics. Springer, Cham. An introduction to set theory and analysis
- Stillwell J (2018) Reverse mathematics. Princeton University Press, Princeton, NJ
- Stirling J (1717) Lineae tertii ordinis Neutoniana. Edward Whistler, Oxford
- Struik D (1969) A source book of mathematics 1200–1800. Harvard University Press, Cambridge
- Taton R (1951) L'œuvre mathématique de G. Desargues. Presses universitaires de France, Paris
- Taurinus FA (1826) Geometriae prima elementa. Cologne
- Taylor B (1715) Methodus incrementorum directa et inversa. William Innys, London
- Thurston WP (1997) Three-dimensional geometry and topology, vol 1. Princeton University Press, Princeton, NJ. Edited by Silvio Levy
- Tietze H (1908) Über die topologische Invarianten mehrdimensionaler Mannigfaltigkeiten. Monatsh Math Phys 19:1–118
- Torricelli E (1643) De solido hyperbolico acuto. Partial English translation in Struik (1969)
- Torricelli E (1645) De infinitis spirabilibus. Reprint edited by E. Carruccio, Domus Galiaeana, Pisa 1955
- Turing A (1936) On computable numbers, with an application to the Entscheidungsproblem. Proc Lond Math Soc ser 2(42):230–265
- Turnbull HW (1939) James Gregory (1638–1675). University of St. Andrews James Gregory Tercentenary, St. Andrews. G. Bell and Sons, London
- Turnbull HW (1960) The correspondence of Isaac Newton, vol II, pp 1676–1687. Cambridge University Press, New York

- Ulam S (1930) Zur Masstheorie in der allgemeinen Mengenlehre. *Fund Math* 15:140–150
- Van Brummelen G (2009) *The mathematics of the heavens and the earth*. Princeton University Press, Princeton, NJ
- Van Brummelen G (2013) *Heavenly mathematics*. Princeton University Press, Princeton, NJ
- van der Waerden B (1976) Pell's equation in Greek and Hindu mathematics. *Russ Math Surveys* 31(5):210–225
- van der Waerden BL (1949) *Modern algebra*. Frederick Ungar, New York
- van der Waerden BL (1954) *Science awakening*. P. Noordhoff Ltd., Groningen. English translation by Arnold Dresden
- van der Waerden BL (1983) *Geometry and algebra in ancient civilizations*. Springer, Berlin
- van Heijenoort J (1967) *From Frege to Gödel. A source book in mathematical logic, 1879–1931*. Harvard University Press, Cambridge, Mass
- Vandermonde A-T (1771) *Mémoire sur la résolution des équations*. *Hist Acad Roy Sci*
- Viète F (1579) *Universalium inspectionium ad canonem mathematicum liber singularis*
- Viète F (1591) *De aequationum recognitione et emendatione*. In his *Opera*, pp 82–162. English translation in Viète (1983)
- Viète F (1593) *Variorum de rebus mathematicis responsorum libri octo*. In his *Opera*, pp 347–435
- Viète F (1615) *Ad angularium sectionum analyticen theoremata*. In his *Opera*, pp 287–304
- Viète F (1983) *The analytic art*. The Kent State University Press, Kent, OH. *Nine studies in algebra, geometry and trigonometry from the Opus Restitutae Mathematicae Analyseos, seu Algebra Nova*, translated by T. Richard Witmer
- Vitali G (1905) *Sul problema della misura dei gruppi di punti di una retta*. Bologna
- von Neumann J (1923) *Zur Einführung der transfiniten Zahlen*. *Acta lit acad sci Reg U Hungar Fran Jos Sec Sci 1*: 199–208. English translation in van Heijenoort (1967) 347–354

- von Neumann J (1930) Letter to Gödel, 20 November 1930, in ?, p 337
- Wagon S (1985) *The Banach-Tarski Paradox*. Cambridge University Press, Cambridge, With a foreword by Jan Mycielski
- Wallis J (1655a) *Arithmetica infinitorum*. Opera 1:355–478. English translation *The Arithmetic of Infinitesimals* by Jacqueline Stedall. Springer, New York, 2004
- Wallis J (1655b) *De sectionibus conicis*. Opera 1:291–354
- Wallis J (1657) *Mathesis universalis*. Opera 1:11–228
- Wallis J (1659) *Tractatus duo. Prior, de cycloide. Posterior, de cissoid*. Opera 1:489–569
- Wallis J (1663) *De postulato quinto; et definitione quinta Lib. 6 Euclidis*. Opera 2:669–678
- Wantzel PL (1837) *Recherches sur les moyens de reconnaitre si un problème de géométrie peut se résoudre avec la règle et le compas*. J Math 2:366–372
- Weeks JR (1985) *The shape of space*. Marcel Dekker Inc, New York
- Weierstrass K (1863) *Vorlesungen über die Theorie der elliptischen Funktionen*. Mathematische Werke 5
- Weierstrass K (1874) *Einleitung in die Theorie der analytischen Funktionen*. Summer Semester 1874. Notes by G. Hettner. Mathematisches Institut der Universität Göttingen
- Weil A (1975) *Introduction to Kummer* (1975)
- Weil A (1976) *Elliptic functions according to Eisenstein and Kronecker*. Springer, Berlin. *Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 88*
- Weil A (1984) *Number theory. An approach through history, from Hammurapi to Legendre*. Birkhäuser Boston Inc, Boston, MA
- Wessel C (1797) *Om Directionens analytiske Betegning, et Forsøg anvendt fornemmelig til plane og sphæriske Polygoners Opløsning*. Danske Selsk Skr N Samml 5. English translation in Smith (1959), vol 1, pp 55–66
- Wessel C (1797) *Om Directionens analytiske Betegning, et Forsøg anvendt fornemmelig til plane og sphæriske Polygoners Opløsning*. Danske Selsk Skr N Samml 5. English translation in Smith (1959), vol 1, pp 55–66
- Whitehead AN, Russell B (1910) *Principia mathematica*. Cambridge University Press, Cambridge. 3 vols. 1910, 1912, 1913

- Whiteside DT (1961) Patterns of mathematical thought in the later seventeenth century. *Arch History Exact Sci* 1:179–388 (1961)
- Whiteside DT (1964) Introduction to The mathematical works of Isaac Newton, vol I. Johnson Reprint Corp, New York, 1964
- Wiles A (1995) Modular elliptic curves and Fermat's last theorem. *Ann Math* (2) 141(3):443–551
- Woodin WH (1999) The axiom of determinacy, forcing axioms, and the nonstationary ideal. Walter de Gruyter & Co, Berlin
- Wright L (1983) Perspective in perspective. Routledge and Kegan Paul, London
- Wussing H (1984) The genesis of the abstract group concept. MIT Press, Cambridge, MA, Translated from the German by Abe Shenitzer
- Yáng Huí (1261) Compendium of analyzed mathematical methods in the “Nine Chapters”
- Zermelo E (1904) Beweis dass jede Menge wohlgeordnet werden kann. *Math Ann* 59:514–516. English translation in van Heijenoort (1967)
- Zeuthen HG (1903) Geschichte der Mathematik im 16. und 17. Jahrhundert. Teubner, Leipzig. Johnson Reprint Corp., New York, 1977
- Zhū Shijié (1303) Siyuan yujian. French translation in Hoe (1977)

Index

A

Abel

- and abelian groups, 265
- and elliptic functions, 157, 177
- and modular functions, 78
- and the quintic, 78
- lemniscate division theorem, 179

addition of points

- on elliptic curve, 220

addition theorem, 167, 173

- and addition of points, 221
- for arcsine integral, 176
- for elliptic integral, 175
- for exponential function, 208
- for lemniscatic integral, 175
- for lemniscatic sine, 179
- for sine, 173

Adyan, 295

affinity, 273

al-Haytham, 126, 237, 248

al-Khwārizmī, 64

- solution of quadratic, 69

Alberti, 100

aleph, 328

algebra, 64

- abstract, 257
- and algebraic geometry, 65
- and polynomial equations, 64
- commutative, 297
- linear, 14, 298
- origin of word, 64

algebraic

- curve, 32, 89
- real, 193

function, 125, 146

- definition, 150

field, 318

fractional power series, 150

power series, 146

geometry, 14, 29

- origin, 65

integer, 306

number, 304

number fields, 303

number theory, 297

- and construction problems, 24

numbers

- form countable set, 325, 326

algebraic geometry, 14, 86

- and algebra, 65

and projective geometry, 95

discovery, 87

algorithm

- Euclidean, 39

origin of word, 64

theory, 295, 323

analysis situs *see* topology, 284

analytic geometry, 87, 97

- and foundations, 97

anamorphosis, 103

angle division, 75

- and complex numbers, 185

de Moivre formula, 76

Leibniz formula, 76

Newton formula, 76

Viète formulas, 76

angular defect, 240

anthyphairesis, 43

and continued fractions, 45
 antiderivative, 138
 Apéry, 154
 Apollonius
 and conic sections, 86
 epicycles, 31
 four-line problem, 87
 theory of irrationals, 71
 arc length, 88, 226
 and elliptic integrals, 170
 integral, 144, 228
 of catenary, 230
 of circle, 144
 of cycloid, 227
 of lemniscate, 171
 of logarithmic spiral, 227
 of semicubical parabola, 227
 Archimedes
 and geometric series, 140
 and Pell's equation, 45
 and volume of sphere, 127
 area of parabola, 51, 60, 123
 cattle problem, 45
 Method, 53, 126
 results on the sphere, 60
 spiral, 128
 area
 of circle, 57
 of hyperbola, 62
 of hyperbolic circle, 240
 of parabola, 60
 of polygons, 58
 of sphere, 60
 of triangle, 56
 proportional to square, 57
 Argand, 190
 Aristotle
 Prior Analytics, 13
 version of Zeno, 52
 arithmetic–geometric mean, 178
 and Gauss, 178
 and Lagrange, 178
 arithmetization
 of geometry, 96, 316

 of syntax, 341
 associative law, 258, 308
 asymptotic lines, 238
 axiom of choice, 331
 and continuous functions, 333
 implies well-ordering, 332
 in measure theory, 332
 statement, 331
 axiom of foundation, 346
 axioms, 17, 18
 choice, 331
 for groups, 258
 in Euclid's *Elements*, 18, 225
 large cardinal, 331
 of infinity, 344
 of set theory, 328, 331, 343
 parallel, 17, 225, 237

B

Bachet
 Diophantus, 158
 edition of Diophantus, 157
 stated four-square theorem, 37
 Banach, 332
 Banach–Tarski theorem, 332
 Beeckman, 94
 Beltrami, 234
 conformal models, 248
 half-space model, 251
 hyperbolic plane, 241
 Berkeley, 53
 Bernays, 342
 Bernoulli
 definition of geodesic, 235
 Jakob
 and elliptic integrals, 171
 and logarithmic spiral, 229, 230
 lemniscate, 30, 171
 Johann
 and $\sum 1/n^2$, 152
 and complex logarithms, 206
 and complex numbers, 186
 and tractrix, 230
 Bessel, 178, 212

Bézout's theorem, 85, 94, 96, 99
 and fundamental theorem
 of algebra, 193, 195
 homogeneous formulation, 120
 stated by Newton, 95
 binomial
 coefficient, 79, 149
 as number of combinations, 80
 divisibility property, 83
 sum property, 81
 series, 149
 theorem, 123, 132, 146
 and Fermat's little theorem, 83
 and interpolation, 147
 Bolyai hyperbolic geometry, 243
 Bolzano, 191
 intermediate value
 theorem, 191, 324
 Bombelli, 157, 183
 Bonnet, 236
 Boole, 339
 Borel, 330
 Bosse, 105
 Brahana, 289
 Brahmagupta
 and Pell's equation, 45
 quadratic formula, 68
 branch point, 200
 Briggs, 148
 Bring, 78
 Brouncker, 132
 and Pell's equation, 43
 continued fraction, 132
 Brunelleschi, 100

C

calculus, 87, 123, 124
 and differential geometry, 226
 and interpolation, 148
 and mechanics, 124
 and method of exhaustion, 124
 and tangents, 124
 fundamental theorem, 137
 of Leibniz, 136

 of Newton, 124, 133
 priority dispute, 136
 Cantor
 continuum hypothesis, 328
 defined $\aleph_0, \aleph_1, \aleph_2, \dots$, 328
 discovered uncountability, 325
 first uncountability proof, 325
 limit point operation, 326
 ordinal generating operations, 327
 transcendental numbers, 326
 Cardano, 73
 and complex numbers, 76, 183
 solution of cubic, 74
 cardinality, 327
 cardinals, 328
 $\aleph_0, \aleph_1, \aleph_2, \dots$, 328
 large, 331, 332
 uncountable, 328
 cardioid, 33
 Cassini, 30
 Cassini oval, 30
 catenary
 and tractrix, 228, 230
 arc length, 230
 cattle problem, 45
 Cauchy
 and permutation groups, 267
 integral theorem, 205, 212
 notation for identity, 267
 notation for inverse, 267
 polygonal number theorem, 37
 Cauchy–Riemann equations, 205, 209
 and hydrodynamics, 208
 Cavalieri
 and volume of sphere, 127
 integration formula, 126
 method of indivisibles, 126
 Cayley
 abstract group concept, 267
 and projective geometry, 273
 permutation group theorem, 268
 projective model, 247
 Chaitin incompleteness theorem, 342
 choice function, 331

- chord–tangent construction, 7, 47, 157, 165
- Church, 338
- circle division, 25, 179
- circular functions
 - and complex logarithms, 206
 - and complex numbers, 186
 - and cubic equations, 75
 - and elliptic functions, 168
 - and the circle, 168
 - partial fraction series, 216
- circumradius, 22
- cisoid, 29
 - cuspid, 89
- classification
 - of surfaces, 287
- Clebsch, 165, 170
 - addition of points, 220
- Cohen, 328
- combinatorics, 124
- common notions, 19
 - and equivalence relations, 20, 275
- commutative law, 308
- complex curves
 - and Newton–Puiseux theory, 203
 - as Riemann surfaces, 198
 - topology, 201
- complex functions, 206
 - and differentiability, 209
 - and integration, 212
 - as power series, 209
 - real and imaginary parts, 208
- complex numbers, 181
 - and angle division, 185
 - and circular functions, 186
 - and cubic equations, 76, 183
 - and elliptic functions, 168, 177
 - conjugate, 190
 - geometric properties, 190
 - geometric representation
 - by Argand, 191
 - by Cotes, 187
 - by Wessel, 191
- composition of functions, 258
- computability, 323, 335
 - and diagonal argument, 334
 - by Turing machine, 335
 - of functions, 336
 - of real numbers, 338
- computably enumerable set, 340
- computation, 323
 - and randomness, 342
- conformal mapping, 205
 - and mapmaking, 210
- conformal model, 248
 - as part of \mathbb{C} , 254
 - disk, 249
 - half-plane, 249
 - distance, 250
 - hemisphere, 248
 - in half-space, 251
- congruence
 - and groups of motions, 272
 - modulo n , 259
 - modulo an irreducible polynomial, 312
- conic sections, 17, 26
 - attributed to Menaechmus, 27
 - in Descartes, 26
 - meaning of names, 26
 - projective view, 99, 110
 - second-degree equations, 85, 87
- conjugates, 190
- constructible
 - number, 26, 315
 - has degree 2^k , 316
 - points, 70
 - polygons, 25
- construction
 - of equations, 94
 - ruler and compass, 17, 23
 - of double circle arc, 173
 - of double lemniscate arc, 174
- continued fraction
 - and Pell’s equation, 45
 - definition, 46

- for π , 132
 - periodic, 47
- continuity, 190
 - and axiom of choice, 333
- continuous
 - functions, 191
 - extreme value theorem, 191
 - intermediate value theorem, 191
 - magnitude, 55
 - Dedekind definition, 55
 - process, 3
- continuum hypothesis, 328, 333
 - consistency, 328
 - independence, 328
- coordinates, 1, 6, 13, 85
 - in Hipparchus, 86
 - in Oresme, 86
 - in vector space, 300
- coset, 261
 - multiplication, 262
- Cotes, 187
 - and complex logarithms, 207
 - and complex numbers, 187
 - Harmonia mensurarum*, 207
 - theorem on n -gon, 187
- countability, 325
- countable additivity, 330
- counting board, 66
- covering, 200
 - of orientable surface, 291
 - of projective plane, 290
 - of pseudosphere, 290
 - of torus, 290
 - projection map, 202
 - sheets of, 200
 - and integration, 215
 - universal, 290
- Cramer
 - and Bézout's theorem, 96
 - and permutations, 266
- Cramer's rule, 66, 298
- cross-ratio, 99
 - and hyperbolic distance, 273
 - as a group invariant, 273
 - in Desargues, 105
 - in Pappus, 106
 - invariance, 115, 117
 - Möbius invariance proof, 107
 - on finite projective line, 280
- cryptography
 - and Fermat's little theorem, 82
- cube, 21
 - duplication of *see* duplication of the cube, 24
 - rotation group, 269
- cubic curves, 29, 85
 - as tori, 203
 - five types, 92, 99
 - geometric features, 85, 89
 - isomorphic to \mathbb{C}/Λ , 218
 - Newton classification, 91
 - of genus 0, 163
 - parameterization, 165, 169
 - projective classification, 221
 - projective view, 110
- cubic equations, 63, 73
 - and circular functions, 75
 - and complex functions, 206
 - and complex numbers, 76, 183
 - and trisection, 75
 - have real roots, 183
 - in Cardano, 74
 - in Viète, 75
 - solution, 73
- curvature, 124
 - center of, 230
 - constant
 - surface of, 225, 245
 - Gaussian, 225, 233
 - geodesic, 236
 - intrinsic, 232
 - negative
 - and non-Euclidean geometry, 225, 234
 - surface of, 225, 233
 - Newton formula, 230
 - of plane curves, 229

- of surfaces, 232
 - principal, 232
 - radius of, 230
- curve
 - algebraic, 32, 89, 193, 226
 - behavior at infinity, 108
 - cubic, 29, 91
 - degree, 89
 - equidistant, 247
 - in conformal model, 249
 - geometric, 89
 - mechanical, 87, 89, 226, 228
 - on projective plane, 113
 - projective, 108
 - transcendental, 89, 226
 - and differential geometry, 226
- cusp, 85, 89
 - of cissoid, 29, 89
 - of semicubical parabola, 92
- cycloid, 32
 - arc length, 227
 - is own involute, 230
 - pendulum, 230
- D**
- d'Alembert
 - and complex functions, 208
 - and conjugate solutions, 190
 - fundamental theorem of
 - algebra, 190
 - lemma, 191
 - on algebra in geometry, 91
- de Moivre
 - formula, 76
 - inversion formula, 135
 - solution by radicals, 76
- Dedekind
 - and algebraic number fields, 303
 - cut, 55, 191, 324
 - for irrational, 55
 - for rational, 55
 - definition of $\sqrt{2}$, 55
 - definition of continuity, 55
 - definition of ideal, 318
 - dimension theorem, 313
 - rigor, 53
 - rings, 322
 - tribute to Kummer, 317
- degree
 - of algebraic number, 305
 - of curve, 17, 85, 89
- Dehn
 - and hyperbolic geometry, 295
 - combinatorial group theory, 278
 - solved Hilbert's third problem, 58
- Desargues, 103
 - and cross-ratio, 105
 - Brouillon projet*, 105
 - projective geometry, 105
 - theorem, 99, 105
 - and foundations, 106
 - statement, 106
- Descartes, 85
 - and algebraic geometry, 13, 87
 - coordinate method, 19
 - factor theorem, 79, 189
 - folium, 89
 - Géométrie*, 87
 - integration formula, 126
 - notation for powers, 79
 - polyhedron formula, 285
- descriptive geometry, 104
- determinant, 66, 120, 298
 - theory, 299
 - and algebraic integers, 306
- diagonal argument, 334
 - and computability, 334
 - and Gödel's theorem, 339
 - and rate of growth, 334
 - for real numbers, 334
 - for sets, 334
- differentiability, 205
- differential equations
 - for geodesics, 235
- differential geometry, 226
 - and calculus, 226
 - and curvature, 229
 - and hyperbolic geometry, 244

- differentiation, 124
- dimension of vector space, 300, 314
 - and basis, 301
 - over \mathbb{Q} , 304, 315
- Diocles, 29
- Diophantine
 - equations, 7, 35
 - cubic, 48
 - linear, 42
 - no algorithm, 7, 36
 - quadratic, 43
 - rational solutions, 7
 - problems, 7
- Diophantus, 4, 35
 - and Diophantine problems, 7
 - and Pythagorean triples, 8
 - chord and tangent methods, 65, 157
 - chord method, 47, 48
 - on folium, 90
 - method, 7
 - and elliptic functions, 165
 - and Fermat, 7
 - and Newton, 7
 - geometric interpretation, 48
 - tangent method, 47, 48, 129
 - and Viète, 49
- Dirichlet
 - function, 329, 331
 - principle
 - and Riemann mapping theorem, 211
 - justified by Hilbert, 211
- discrete process, 3
- distance, 97
 - and Pythagorean theorem, 13
 - definition of, 97
- distributive law, 308
- divergence of harmonic series, 141
- divisibility
 - and Pythagorean triples, 5
 - in Euclid, 5
- division of stakes, 80
- dodecahedron
 - rotation group, 270
- double periodicity, 178
 - and complex integration, 215
 - and Riemann, 178, 215
 - of Weierstrass \wp -function, 217
- double point, 89, 163
- double root, 164
- doubling the arc
 - of circle, 173
 - of lemniscate, 173, 174
- du Bois-Reymond, 334
- duplication of the cube, 17, 24
 - by cissoid, 29
 - by intersecting conics, 27
 - by Menaechmus, 27
- Dürer, 100
- Dyck
 - concept of group, 268
 - groups and tessellations, 271
- E**
- e is transcendental, 25
- Eisenstein
 - and algebraic integers, 306
 - series, 216
- elastica, 170
- elimination, 65, 95
 - and linear algebra, 120
 - and polynomial equations, 66
 - Gaussian, 65
- ellipse, 26
 - arc length, 157, 170
 - as planetary orbit, 27
 - versus Cassini oval, 30
 - focus of, 28
 - not an elliptic curve, 170
 - string construction, 28
- elliptic
 - curves, 36, 157, 167, 170, 218
 - addition of points, 220
 - and Fermat's last theorem, 158, 218
 - isomorphic to \mathbb{C}/Λ , 220

- parameterized by \wp, \wp' , 220
- functions, 38, 87, 138, 157, 165, 170
 - addition theorem, 167
 - and complex numbers, 177, 205
 - and the torus, 203
 - birth day, 175
 - by inverting integrals, 177
 - double periodicity, 178, 215
 - series expansions, 216
- integrals, 157, 170
 - addition theorem, 175
 - not elementary, 171
- elliptic modular functions *see* modular functions, 78
- empty set, 327
- epicycles, 31
- equation
 - cubic, 73
 - solution, 73
 - Diophantine, 35
 - equation, 63
 - linear, 63, 65
 - modular, 280
 - Pell's, 35, 43
 - polynomial, 64
 - quadratic, 63
 - Brahmagupta formula, 64
 - in Babylon, 64
 - in Euclid, 64
 - quartic, 77
 - quintic, 63, 78
- equivalence relation, 20
 - defined by group, 275
- Euclid, 4
 - Elements*, 4, 17
 - Book V, 51, 54
 - common notions, 19, 275
 - postulates, 18
 - perfect number theorem, 38
 - and geometric series, 61
 - proofs of Pythagorean theorem, 11
 - Pythagorean triples formula, 4
 - theory of divisibility, 5
 - theory of irrationals, 71
 - used induction, 41
 - view of quadratic equations, 64
- Euclidean
 - algorithm, 35, 39
 - for Gaussian integers, 310
 - for polynomials, 168, 309
 - geometry, 97
 - on horosphere, 244
 - on torus, 292
 - plane, 97
 - rigid motions, 253
 - tessellations, 252
- Eudoxus, 51
 - definition of equality, 54
 - method of exhaustion, 56
 - theory of proportions, 54
- Euler
 - addition theorems, 167, 175
 - and Bézout's theorem, 96
 - and chord–tangent construction, 165
 - and complex logarithms, 207
 - and conformal mapping, 210
 - characteristic, 283, 285
 - and genus, 289
 - Poincaré generalization, 286
 - constant, 142
 - and zeta function, 155
 - continued fraction formula, 133
 - cotangent series, 216
 - formula for e^{ix} , 207
 - geodesic differential equation, 235
 - pentagonal number theorem, 37
 - perfect number theorem, 38
 - polyhedron formula, 285
 - Legendre proof, 285
 - product formula, 153
 - proof of Fermat's little theorem, 83, 257
 - summed $\sum 1/n^2$, 151
 - used algebraic integers, 308
 - values of $\zeta(s)$, 154

zeta function formula, 139, 153
 exhaustion *see* method of exhaustion, 56
 exponential function, 135
 addition formula, 208
 complex, 205, 207
 periodicity, 205, 207
 extreme value theorem, 191, 192

F

factor theorem, 79, 152
 Fagnano, 165
 addition theorem, 167
 duplication formula, 174
 and modular equations, 280
 studied by Euler, 175
 lemniscate division, 179
 Fermat, 85, 157
 and algebraic geometry, 13, 87
 and Diophantus, 48
 and Diophantus's method, 7
 and rational right triangles, 159
 infinite descent, 159
 integration formula, 126
 last theorem, 158
 and elliptic curves, 218
 attempt by Lindemann, 25
 for $n = 4$, 159
 little theorem, 82, 257
 proof using inverses, 260
 Observations on Diophantus, 158
 tangent method, 128
 applied to folium, 128
 Ferrari, 73
 solution of quartic, 77
 Fibonacci
 and cubic irrationals, 71
 field, 72, 265, 297
 algebraic number, 303
 and vector space, 301
 as vector space, 303, 311
 axioms, 302
 finite, 280, 303

 generated by algebraic number, 305
 of algebraic functions, 318
 of all algebraic numbers, 313
 of congruence classes mod p , 303
 of congruence classes mod $p(x)$, 312
 of finite dimension over \mathbb{Q} , 315
 Fior, 73
 focus, 28
 in astronomy, 29
 folium
 asymptote, 90
 double point, 89
 drawn by Huygens, 90
 has genus 0, 163
 of Descartes, 89
 parameterization, 90
 tangent of, 128
 foundations
 arithmetic and set-theoretic, 54
 geometric, 54
 of geometry, 106
 four-square theorem, 37
 Fourier, 329
 Frege, 339
 Friedman, 345
 function
 algebraic, 138, 146
 choice, 331
 computable, 336
 continuous, 191
 differentiable, 205
 Dirichlet, 329, 331
 elementary, 170
 elliptic, 138
 linear fractional, 259
 many-valued, 149, 205, 214
 modular, 78, 178
 rational, 146
 symmetric, 264
 theta, 38, 178
 transcendental, 138
 zeta, 153
 fundamental group, 283, 294

- as group of motions, 294
- defined by Poincaré, 295
- generators and relations, 283, 295
- of sphere, 283
- of torus, 283
- fundamental polygon, 288
 - and universal covering, 291
 - for genus 2, 292
 - for torus, 291
- fundamental theorem
 - of algebra, 181, 189
 - and Bézout's theorem, 193, 195
 - and intersections, 195
 - d'Alembert proof, 190
 - Gauss proofs, 190
 - Kronecker version, 313
 - motivated by integration, 188
 - real version, 190
- of arithmetic, 41
- of calculus, 137
 - generalized, 213
 - in Leibniz formalism, 137

G

Galois

- and modular equations, 280
- and normal subgroups, 262, 265
- and the quintic, 78, 266
- discovered finite fields, 280, 303
- discovered simple groups, 279
- introduced group concept, 257, 265
- theory, 265
 - and regular polyhedra, 22
- theory of fields, 265
- gamma function, 155
- Gauss
 - and circle division, 25
 - and complex integration, 212
 - and conformal mapping, 210
 - and elliptic functions, 177
 - and lemniscate division, 179

- and modular functions, 78, 178
- and the agM, 178
- area of hyperbolic circle, 240
- construction of 17-gon, 25
- curvature, 225, 233
- formula for sphere motion, 254
- fundamental theorem of algebra, 190
- geodesic curvature, 236
- geodesy, 232
- sphere, 198
- theorema egregium*, 233
- triangle tessellation, 255, 292
- used algebraic integers, 308
- Gaussian
 - curvature, 225, 233
 - elimination, 63, 65, 298
- Gaussian integer, 306
 - Euclidean algorithm, 310
 - unique prime factorization, 310
- generators and relations, 271, 275
 - and topology, 277
 - read off tessellation, 277
- genus, 162
 - and Euler characteristic, 289
 - and rational functions, 163
 - as number of holes, 204
 - of algebraic curve, 204, 283
 - topological meaning, 198
- geodesic, 235
 - curvature, 236
 - differential equation, 235
 - mapped to straight line, 245
 - on cone, 236
 - on cylinder, 236
 - on pseudosphere, 236
 - on sphere, 235
- geometric series, 51, 134
 - and area of parabola, 60
 - and volume of tetrahedron, 59
 - in Euclid, 61, 139
- geometry
 - algebraic, 14, 29, 63, 86
 - analytic, 87, 97
 - complex interpretation, 252

- descriptive, 104
 - differential, 226
 - foundations of, 106
 - hyperbolic, 241
 - infinitesimal, 137
 - non-Euclidean, 19, 87, 182, 225, 234
 - of surfaces, 245
 - projective, 95, 99, 104
 - spherical, 240
 - Gödel
 - and continuum hypothesis, 328
 - arithmetization, 341
 - incompleteness theorem, 339
 - and computability, 339
 - “miracle” of computability, 335
 - second theorem, 341
 - in Hilbert and Bernays, 342
 - golden ratio, 26
 - golden rectangle, 21
 - constructibility, 71
 - Goursat, 214
 - Grandi, 91
 - Grassmann
 - and vector spaces, 299
 - and induction, 42
 - and inner product, 14
 - and Steinitz exchange lemma, 301
 - Green, 213
 - Green’s theorem, 213
 - implies Cauchy’s theorem, 213
 - Gregory, 147
 - and interpolation, 148
 - and Taylor’s theorem, 147
 - Gregory–Newton formula, 147
 - group
 - abelian, 262
 - simple, 279
 - alternating, 266
 - associativity, 267
 - cancellation, 268
 - concept of Galois, 265
 - cyclic, 259
 - and radicals, 265
 - simple, 279
 - defining properties, 258
 - fundamental, 283, 294
 - identity, 258
 - inverse, 258
 - isomorphism, 267, 268
 - isomorphism problem, 295
 - of motions, 272
 - of permutations, 265
 - of real projective line, 273
 - of rigid motions, 252
 - of transformations, 257, 272
 - on a cubic curve, 267
 - polyhedral, 269
 - and theory of equations, 271
 - presentation, 271
 - quotient, 262
 - rotation, 269
 - S_n , 263
 - simple, 279
 - smallest nonabelian, 279
 - smallest nonabelian, 278
 - solvable, 265
 - symmetric, 263
 - word problem, 338
 - group theory, 17, 223, 257
 - and theory of equations, 265
 - combinatorial, 275, 276
 - geometric, 276
- ## H
- Hadamard, 187
 - halting problem, 337
 - Hamilton
 - presented icosahedral group, 271
 - handle, 290
 - harmonic series, 139, 141
 - harmony
 - and integer ratios, 12
 - and Pythagoras, 12
 - Harnack, 329
 - Harriot
 - and interpolation, 148

- and logarithmic spiral, 226
 - and stereographic projection, 210
 - theorem on spherical area, 240, 243
 - Hausdorff, 332
 - Heath, 159
 - Hermite
 - followed Galois's hint, 266
 - solution of quintic, 78, 280
 - transcendence of e , 25
 - Heron, 28
 - Heuraet, 227
 - Hilbert
 - foundations of geometry, 97, 106
 - justified Dirichlet principle, 211
 - problems, 58
 - first, 328
 - third, 58
 - rectified flaws in Euclid, 19
 - theorem on constant curvature, 233
 - Hipparchus, 86
 - Hobbes
 - denounced Wallis's *Conics*, 96
 - in love with geometry, 18
 - on *Arithmetica infinitorum*, 131
 - on Torricelli's result, 127
 - Holbein, 103
 - Hölder, 185
 - homeomorphism, 284
 - problem, 295, 338
 - homogeneous coordinates, 118
 - homotopic paths, 294
 - horocycle, 247
 - in conformal model, 249
 - horosphere, 244
 - in half-space model, 251
 - is Euclidean, 244
 - Hudde, 129
 - Huygens
 - and pseudosphere, 233
 - description of tractrix, 228
 - drew folium, 90
 - on discoveries in geometry, 124
 - hydrodynamics
 - and complex functions, 208
 - hyperbola, 26
 - arc length, 170
 - area of segment, 62
 - points at infinity, 108
 - quadrature of, 134
 - hyperbolic
 - circle, 247
 - in conformal model, 249
 - geometry, 241
 - and differential geometry, 244
 - complex interpretation, 255
 - conformal models, 248
 - named by Klein, 241
 - plane, 241
 - as covering, 292
 - rigid motions, 247
 - tessellations, 254
 - space, 250
 - rigid motions, 256
 - tessellation, 293
 - trigonometry, 241
 - hypergeometric, 131
- I**
- icosahedron
 - constructibility, 71
 - Pacioli construction, 21
 - rotation group, 270
 - tessellation, 253
 - ideal numbers, 318
 - ideals, 318
 - containment and division, 319
 - definition of, 318
 - in \mathbb{Z} , 319
 - in $\mathbb{Z}[\sqrt{-5}]$, 320
 - in algebraic geometry, 318
 - maximal, 321
 - prime, 321
 - prime factorization of, 318
 - principal, 319
 - product of, 321

- sum of, 319
- identity, 258
- identity law, 308
- incommensurable *see* irrational, 12
- indivisibles, 126
 - in *Arithmetica infinitorum*, 131
- induction, 41
 - and infinite descent, 41
 - as base step, induction step, 42
 - in Euclid, 41
 - in Grassmann, 42
 - in Pascal, 80
 - proof by, 42
- infinite, 323
 - completed, 52
 - and limits, 52
 - and set theory, 54
 - descent, 159, 161
 - in Greek mathematics, 13, 51
 - potential, 52
 - processes, 51
 - for finding volume, 58
 - rejected by Greeks, 52
 - product, 131, 139, 153
 - reasoning about, 52
 - sequence, 52
 - set of points, 52
- infinite series, 124, 139, 140
 - for algebraic functions, 146
 - for circular functions, 134, 139, 143
 - for log, 135
 - for π , 143
 - in Greek mathematics, 140
 - inversion, 135
 - by de Moivre, 135
 - Newton's calculus of, 124
- infinitesimals, 53, 123, 137
 - of Robinson, 125
 - quotient of, 123, 137
 - sum of, 123, 137
- infinity
 - behavior of curves at, 108
 - inflection at, 110
 - line at, 106
 - point at, 105
- infinity *see* infinite, 51
- inflection, 85, 89, 110
- inner product
 - and angle, 301
 - and length, 301
 - and Pythagorean theorem, 1, 14, 299
 - definition, 301
- inradius, 22
- integral
 - arcsine, 172
 - elliptic, 170
 - Lebesgue, 329
 - lemniscatic, 171
 - Riemann, 329
- integration, 124
 - and arc length, 227
 - and partial fractions, 188
 - complex, 212
 - and Riemann surfaces, 215
 - in "closed form", 138, 170
 - of algebraic functions, 125
- intermediate value theorem, 191
- interpolation, 147
 - and calculus, 148
 - and Taylor's theorem, 147
 - Gregory–Newton formula, 147
- intersections
 - and Bézout's theorem, 95
 - and fundamental theorem of algebra, 195
 - and roots, 27, 94, 193
 - multiplicity, 194
 - of real algebraic curves, 193
- inverse
 - Cauchy notation, 267
 - function, 135, 157
 - in group theory, 258, 268
 - mod p , 259
 - of algebraic number, 305
- inverse law, 308
- involute, 230
- irrational, 1, 3, 12

irrationality of $\sqrt{2}$, 1, 3, 35

irrationals

Dedekind construction, 54

Euclid's theory, 71

quadratic, 71

isometric surfaces, 233

isomorphic groups, 220, 267, 268

isomorphism, 218, 267

preserves structure, 220

J

Jacobi

and chord–tangent construction,
165

and elliptic curves, 218

and elliptic functions, 157, 177

and modular functions, 78

Fundamenta nova, 177

theta functions, 38, 178

Jade Mirror, 66, 67

Jia Xiàn, 80

Jordan

and Lagrange's theorem, 261

and simple groups, 280

book on group theory, 266

measure, 330

K

Kac, 73

Kepler

introduced term “focus”, 28

planetary spheres, 22

Klein

and modular functions, 178

and the quintic, 78

and uniformization, 222

Elementary Mathematics, 301

Erlanger Programm, 257, 273

hyperbolic tessellations, 293

named hyperbolic geometry, 241

Koebe, 222

Kronecker

and algebraic number fields, 303

fundamental theorem, 303, 313

Kummer, 297

and unique prime factorization, 317

ideal numbers, 318

L

Lagrange

and conformal mapping, 210

and epicycles, 31

and permutations, 257

and the agM, 178

four-square theorem, 37

subgroup theorem, 261

theorem on Pell's equation, 45

theory of equations, 264

Lambert

and conformal mapping, 210

imaginary sphere, 240

introduced hyperbolic functions, 240

spherical geometry, 240

Landau, 72

large cardinals, 331

lattice of periods, 218

shape, 221

Laurent, 214

least upper bound

of ordinals, 327

property of \mathbb{R} , 324, 325

Lebesgue, 329

Legendre

and elliptic integrals, 176

Leibniz

and determinants, 298

and formal logic, 339

and function concept, 138

and integral calculus, 167

and interpolation, 148

calculus, 123, 136

first publication on calculus, 136

integral sign, 137

proof of Fermat's little theorem, 83

solution by radicals, 76

Leibniz–de Moivre formula, 76

and logarithms, 206

lemniscate

- arc length, 171
- as spiric section, 30
- division, 179
 - Abel's theorem, 179
- doubling the arc, 173
- of Bernoulli, 171
- lemniscatic
 - integral, 171
 - addition theorem, 175
 - sine, 177
 - addition theorem, 179
 - derivative, 179
 - period, 177
- Leonardo, 103
- Levi ben Gershon, 79
 - and permutations, 263
- limit
 - and completed infinite, 52
 - of a sequence, 52
 - point, 326
 - rotation, 247
- Lindemann, 24, 143
- line at infinity, 106
- linear
 - equations
 - Chinese method, 65
 - Cramer's rule, 66
 - Diophantine, 42
 - Gaussian elimination, 65
 - in the *Nine Chapters*, 65
 - fractional transformations, 115, 117, 223
 - as rigid motions, 256
 - given by three values, 275
 - groups of, 271, 295
 - inverses of, 259
 - of finite projective line, 280
 - of hyperbolic plane, 274
 - realize projections, 117
 - independence, 300
- linear algebra, 14, 298
 - as theory of vector spaces, 299
- Liouville
 - and elliptic integrals, 171
 - and half-plane model, 250
- Listing, 288
- Liu Hui, 65
- Lobachevsky
 - hyperbolic geometry, 243
 - hyperbolic volumes, 244
- logarithm
 - basic property, 62
 - complex, 186, 205, 206
 - and circular functions, 206
 - infinitely many values, 207
 - geometric definition, 62
 - tables, 148
- logic, 323
- M**
- Maclaurin, 96
- Mādhava, 132
- Magnus, 278
- Markov, 295
- Matiyasevich, 7, 43
- measure, 329
 - Borel, 330
 - countable additivity, 330
 - Jordan, 330
 - Lebesgue, 330
 - zero, 330
- mechanics, 124, 170, 228
- Menaechmus, 27
 - and conic sections, 27, 86
 - construction of $\sqrt[3]{2}$, 86
 - duplication of the cube, 27
- Mengoli, 151
- Mercator, 134
 - power series for log, 146, 155
 - projection, 210
- Mercator, Gerard, 210
- Mercator, Nicholas, 210
- Mersenne, 103
 - primes, 38
- method of exhaustion, 13, 51, 56
 - and approximation, 56
 - and area of parabola, 61
 - avoids limits, 58

- generalizes theory of proportions, 56
 - in Euclid, 56
- Minding, 233
 - hyperbolic trigonometry, 241
- minimal polynomial, 305
- Möbius
 - and cross-ratio, 107
 - and surface topology, 204
 - band, 114
 - and nonorientable surfaces, 288
 - classification of surfaces, 287
 - groups of transformations, 273
- modular
 - equation, 280
 - function, 266
 - tessellation, 249
- modular functions, 78, 178
 - and lattice shape, 222
 - and the quintic, 78
 - periodicity, 223, 249
- Mordell theorem, 48
- multinomial coefficient, 84
- multinomial theorem, 83
- multiplicity, 194
 - and Bézout's theorem, 195
- N**
- Neil, 88, 227
- nested interval
 - property of \mathbb{R} , 324
- Neumann, 211
- Newton
 - algebra of infinite series, 133
 - and Bézout's theorem, 95
 - and Diophantus's method, 7, 48
 - and fractional power series, 150
 - and interpolation, 148
 - calculus, 123, 124, 133
 - classification of cubics, 85, 91, 110
 - curvature formula, 230
 - De analysi*, 134
 - De methodis*, 133
 - defined tractrix, 228
 - formula for $\sin n\theta$, 76
 - law of gravitation, 27
 - Principia*, 91
 - sine series, 135
- Newton–Leibniz priority dispute, 136
- Newton–Puiseux theory, 150
 - and algebraic curves, 203
 - and branch points, 200
 - and complex functions, 214
- Nicéron, 103
 - chair, 104
- Nielsen, 295
- Nine Chapters*, 65
- Noether, Emmy, 322
- non-Euclidean geometry,
 - 19, 87, 225
 - and linear fractional transformations, 223
 - and negative curvature, 234
 - and pseudosphere, 234
 - in Saccheri, 239
- nonconstructibility
 - of $\sqrt[3]{2}$, 72, 316
 - due to Wantzel, 72
 - Landau proof, 72
- norm, 316
- normal subgroup, 262, 265
- Novikov, 338
- number
 - algebraic, 304
 - cardinal *see* cardinals, 328
 - complex, 157, 181
 - constructible, 26
 - ideal, 318
 - irrational, 1, 3, 12
 - and theory of proportions, 54
 - Dedekind construction, 54
 - ordinal *see* ordinals, 326
 - pentagonal, 37
 - perfect, 38, 82
 - polygonal, 36
 - prime, 38

- rational, 6, 51
 - real, 51, 191
 - tetrahedral, 82
 - transcendental, 24, 326
 - triangular, 36, 82
- O**
- octahedron, 21
 - rotation group, 270
 - orbit, 274
 - order of a group, 261
 - ordinals, 326
 - and well-ordering, 332
 - generating operations, 327
 - inaccessible, 346
 - ordered by \in , 327
 - uncountable, 327
 - von Neumann, 327
 - Oresme, 86, 139, 140
 - and harmonic series, 141
 - coordinates, 86
 - series summation, 140
 - velocity–time graph, 86
 - orientability, 288
 - Ostrogradsky, 213
 - Ostrowski, 190
- P**
- PA *see* Peano arithmetic, 42
 - Pappus, 106
 - Pappus’s theorem, 99
 - parabola, 26
 - area of segment, 60
 - cartesian, 94
 - point at infinity, 108
 - semicubical, 88, 92, 227
 - parallel axiom, 17, 19, 237
 - alternatives, 238
 - and angle sum, 239
 - and Pythagorean theorem, 239
 - equivalents of, 237
 - Euclid’s version, 237
 - fails in negative curvature, 246
 - parameterization
 - by circular functions
 - of circle, 169
 - by elliptic functions
 - given by Clebsch, 170
 - known to Jacobi, 170
 - of cubic curves, 165, 169
 - by rational functions, 162
 - fails for $y^2 = 1 - x^4$, 167
 - of circle, 163
 - of folium, 163
 - of curves $y^2 = p(x)$, 170
 - Paris–Harrington theorem, 344
 - Pascal
 - triangle, 79, 80
 - in China, 79
 - Peano
 - vector space axioms, 299
 - Peano arithmetic, 42, 341
 - and reverse mathematics, 345
 - Pell’s equation, 35, 43
 - and Archimedes, 45
 - and Brahmagupta, 45
 - and Brouncker, 43
 - and continued fractions, 45
 - and Lagrange, 45
 - pendulum, 170
 - cycloidal
 - and involute, 230
 - pentagon construction, 26
 - periodicity, 157
 - double, 215
 - of complex exponential, 205, 207
 - of modular function, 223
 - permutation, 80, 263
 - cycles, 281
 - even, 266
 - group, 265
 - Cayley’s theorem, 268
 - permutations, 257
 - Perseus, 30
 - perspective, 100
 - Alberti’s veil method, 100
 - depiction of tiled floor, 101
 - \wp -function, 176

- π , 24
 - Brouncker formula, 132
 - infinite series, 132
 - transcendence, 24, 143
 - Viète formula, 131
 - Wallis formula, 131
- Plato, 4
- Plimpton 322, 4, 5
 - and Pythagorean triples, 4
- Poincaré
 - and elliptic curves, 218
 - and elliptic functions, 165
 - and Euler characteristic, 286
 - and non-Euclidean geometry, 223, 225
 - and rational points, 48
 - and uniformization, 222
 - defined fundamental group, 295
 - formulas for hyperbolic motions, 254
 - group theory, 274
 - hyperbolic tessellations, 293
- point
 - at infinity, 95, 105, 112
 - in Desargues, 105
 - in Kepler, 105
 - on projective line, 106
- polygonal
 - number theorem, 37
 - numbers, 36
- polyhedron
 - formulas, 285
 - regular, 17, 20
- polynomial equations, 63
 - and elimination, 66
 - and intersections of curves, 66
 - in the *Jade Mirror*, 66
 - in several variables, 66
- Poncelet, 106
- Post, 335
 - on meaning and truth, 345
 - version of Gödel's theorem, 339
 - before Gödel, 341
- power series, 139, 146
 - and calculus, 124
 - for algebraic functions, 146
 - for complex functions, 205, 209
 - from Cauchy's theorem, 214
 - for cosine, 209
 - for exponential function, 135, 209
 - for log, 146
 - for sine, 135
 - fractional, 149, 214
 - Laurent, 214
- prime
 - algebraic integer, 316
 - divisor property, 39, 40
 - for Gaussian integers, 310
 - in polynomial ring, 309
 - factorization, 41
 - generalization of, 297
 - ideal, 321
- primes, 38, 139
 - infinitely many, 35, 38, 154
 - Mersenne, 38
 - and perfect numbers, 38
 - of form $2^{2^h} + 1$, 36
- Principia Mathematica*, 339
- probability theory
 - and Pascal's triangle, 80
- projective
 - completion
 - of \mathbb{C} , 197
 - of \mathbb{R} , 197
 - geometry, 95, 99, 104
 - and algebraic geometry, 95
 - line, 112, 115
 - as infinite circle, 106, 113
 - complex, 196
 - finite, 280
 - real, 117, 196, 259
 - model, 247
- plane
 - curves on, 113
 - is nonorientable, 114, 288
 - real, 112
 - sphere model, 196
- transformations, 115, 246, 258, 273

pseudosphere, 228, 230
 and horocycles, 247
 by revolving tractrix, 233
 constant negative curvature, 233
 Gaussian curvature, 235
 geodesics, 236, 252
 has hyperbolic trigonometry, 241
 mapped into half-plane, 251
 principal curvatures, 235

Ptolemy, 31

Almagest, 31

epicycles, 31

Puiseux, 150

Pythagoras

and harmony, 12

theorem of, 2

Pythagorean equation, 35

Pythagorean theorem, 1, 2

and arc length, 144

and definition of distance, 13

and distance, 97

and Hobbes, 18

and inner product, 14, 299

and parallel axiom, 239

converse, 2

proof, 10

proof from “right axiom”, 345

Pythagorean triples, 1, 4

and divisibility, 5

formula, 4

in Diophantus, 8

in Euclid, 4

in Babylon, 4, 12

in Plimpton 322, 4

of rational functions, 168

rational, 6

Q

quadratic

equations, 68

in al-Khwārizmī, 69

in Babylon, 68

in Brahmagupta, 68

in Euclid, 69

forms, 88

formula, 64

irrationals, 71

quadrature, 24, 134

quartic equations, 77

quintic equations, 63, 78

and group theory, 257, 265

and simple groups, 279

R

\mathbb{R} , 324

completeness property, 324, 325

least upper bound property, 324, 325

measurability of subsets, 331

implies large cardinals, 332

nested interval property, 324

uncountability, 325

measure theory proof, 331

well-ordering, 332

radical, 257, 264

Ramsey theorem, 344

rank, 346

rational

function

parameterization, 162

numbers, 6, 13

form countable set, 325

points, 6

on cubic curve, 48, 157

on curve of degree 2, 162

on curve of genus 0, 162

on curve of genus 1, 165

on the circle, 6

on the folium, 164

Pythagorean triples, 6

right triangles, 158

solutions, 7

recurrence relations

and $\sqrt{2}$, 43, 53

recursively enumerable set, 340

regular

polygon, 21

polyhedra, 20

and finite groups, 22

- and Galois theory, 22
 - rotation groups, 269
- resultant, 95, 120
 - as a determinant, 120
- reverse mathematics, 345
- rhumb line, 226
- Riemann
 - and double periodicity, 178, 215
 - and Euler characteristic, 286
 - and genus, 204, 283
 - distance formula, 250
 - functional equation for $\zeta(s)$, 155
 - hypothesis, 154
 - integral, 329
 - mapping theorem, 211
 - surface, 198, 204, 288
 - and complex integration, 215
 - is orientable, 288
 - tessellations, 255
 - theory of elliptic functions, 215
 - zeta function, 154
- rigid motions, 235
 - as linear fractional transformations, 256
 - group of, 252
 - of Euclidean plane, 253
 - of hyperbolic plane, 246, 247, 273
 - of hyperbolic space, 256
 - of sphere, 253
 - of tessellation, 294
- ring, 297, 308
 - axioms, 308
 - Dedekind, 322
 - polynomial, 308
- Roberval, 88, 126
- rope stretching, 2
- roses of Grandi, 91
- rotations, 247, 269
 - and groups, 269
 - of polyhedra, 269
- Ruffini, 78
- ruler and compass construction, 23
 - of points, 70
 - of regular 17-gon, 25
 - of regular pentagon, 26
 - of square root, 24
- Russell, 339
- S**
- Saccheri, 238
- saddle, 233
- Salmon, 221
- Schwarz
 - and Riemann mapping theorem, 211
 - and universal covering, 291
 - tessellations, 225, 255
- Scipione del Ferro, 73
- Seifert and Threlfall, 295
- Seki, 298
- Set theory, 54, 323
 - and completed infinite, 54
 - and large cardinals, 332
 - history, 333
- sets, 323
 - and mathematical objects, 339
 - and real numbers, 324
 - Borel, 330
 - computably enumerable, 340
 - countable, 325
 - nonmeasurable, 332
 - uncountable, 328
- sheets, 200
- side and diagonal numbers, 43
- similarity, 273
- Sluse, 129
- solution by radicals, 78, 264
- sphere
 - tessellations, 253
 - volume and area, 60
- spherical geometry, 240
 - imaginary, 240
 - triangles, 240
- spira, 30
- spiral
 - equiangular, 226
 - logarithmic, 226
 - is own involute, 230

- self-similarity, 229
- of Archimedes, 128
- spiric sections, 30
- squaring the circle, 17, 24, 143, 226
- stereographic projection, 197
 - and conformal models, 248
 - conformality, 210
 - due to Harriot, 210
 - due to Ptolemy, 210
 - preserves circles, 210
- Stevin, 308
- Stirling, 92
- subgroup, 259
 - normal, 262
- Suiseth, 140
- sums of squares, 36
- surface
 - closed, 287
 - compact, 287
 - covering, 290
 - curvature, 232
 - nonorientable, 288
 - normal form, 287
 - of constant curvature, 225
 - Hilbert theorem, 233
 - orientable, 288
 - Riemann, 215, 288
- symmetry, 264
 - geometric, 272
 - in equivalence relation, 20, 275
 - of tessellations, 268

T

- tangent method
 - of Diophantus, 47, 129
 - of Fermat, 128
 - of Hudde and Sluse, 129
- Tarski, 332
- Tartaglia, 73
- Taurinus, 240
- Taylor series, 147
- tessellations
 - groups of, 271, 275

- of Euclidean plane, 252
- of hyperbolic plane, 254
- of sphere, 253, 271
- tetrahedron, 21
 - Euclid's dissection, 59
 - rotation group, 269
 - volume, 58
 - in Euclid, 51, 58
- Thales, 18
- theory of equations, 78, 263
- theory of proportions, 13, 51, 54
 - and irrational numbers, 54
 - in Euclid, 54
- theta functions, 38, 178
- Thurston, 284
- Tietze, 295
- tiled floor, 101
- topology, 182, 223, 283
 - and group theory, 277
 - and regular polyhedra, 286
 - combinatorial structures, 284
 - general, 284
 - geometric, 284
 - in Erlanger Programm, 284
 - of complex curves, 201
 - of surfaces, 204
- Torricelli, 126
 - and logarithmic spiral, 227
 - infinite solid, 141
- torus, 203
 - and cubic curves, 203
 - and elliptic functions, 168, 203, 205
 - and spiric sections, 30
 - as space of equivalence classes, 218
 - constructed by pasting, 219
 - Euclidean geometry, 292
 - fundamental group, 283
 - fundamental polygon, 291
 - integration on, 215
 - nonbounding curves, 215
- tractrix, 228
 - constant tangent property, 228
 - is involute of catenary, 230
 - parametric equations, 231

transcendence, 24
 Cantor proof, 326
 of e , 25
 of π , 24, 143
 transcendental
 curve, 89
 function, 138, 146
 number, 24, 326
 transformations
 continuous, 273
 invertible, 284
 group of, 257, 272
 in Möbius, 273
 linear fractional *see* linear
 fractional transformations,
 115
 projective, 105, 259
 translation, 247
 transposition, 266
 trigonometric series, 326
 and integrals, 329
 trisection, 17, 24
 and cubic equations, 75
 Turing, 335, 338
 machine, 335
 universal, 337
 unsolvability of halting problem,
 337

U
 Ulam, 332
 uncountability, 325
 of ordinals, 327
 uniformization, 222
 unique prime factorization, 35, 83,
 154, 297
 and Kummer, 317
 failure in algebraic integers, 317
 for Gaussian integers, 310
 in polynomial ring, 309
 of ideals, 322
 unsolvability, 323, 337
 in Diophantine equations, 7
 in group theory, 295, 338

 in logic, 338
 in topology, 295

V
 van Heuraet, 88
 Vandermonde, 264
 vanishing point, 101
 vector space, 72, 297
 axioms, 299
 basis, 300
 dimension, 300
 Euclidean, 299
 over a field, 304
 velocity–time graph, 86
 Viète, 75
 and Diophantus, 49
 formula for $\cos n\theta$, 76
 product formula, 131
 solution of cubic, 75
 Vitali, 332
 volume, 58
 of sphere, 60, 127
 of tetrahedron, 58
 in Euclid, 58
 von Neumann, 327

W
 Wachter, 244
 Wallis
 and parallel axiom, 237
 Arithmetica infinitorum, 130
 arithmetized geometry, 96
 infinite product formula, 131
 product, 153
 Wantzel, 24
 and $\sqrt[3]{2}$, 72
 Weierstrass
 extreme value theorem, 191
 intermediate value theorem, 191
 \wp -function, 176, 216
 double periodicity, 217
 rigor, 53
 well-ordering, 332
 Whitehead, 339

word problem, 338

Wren, 227

Y

Yáng Huí, 80

Z

Zeno

and infinite series, 140

paradoxes, 52, 324

Zermelo, 332

incompleteness theorem, 346

well-ordering theorem, 332

Zermelo–Fraenkel axioms, 343

zeta function, 153

Euler formula, 153

functional equation, 155

Riemann, 154

trivial zeros, 154, 155

values found by Euler, 154

Zeuthen, 159

Zhū Shijié, 66, 80

\mathbb{Z}_n , 259